Problems on q-Analogs in Coding Theory

Tuvi Etzion*

May 28, 2013

Abstract

The interest in q-analogs of codes and designs has been increased in the last few years as a consequence of their new application in error-correction for random network coding. There are many interesting theoretical, algebraic, and combinatorial coding problems concerning these q-analogs which remained unsolved. The first goal of this paper is to make a short summary of the large amount of research which was done in the area mainly in the last few years and to provide most of the relevant references. The second goal of this paper is to present one hundred open questions and problems for future research, whose solution will advance the knowledge in this area. The third goal of this paper is to present and start some directions in solving some of these problems.

*Department of Computer Science, Technion, Haifa 32000, Israel, e-mail: etzion@cs.technion.ac.il.
[1]This research was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q^n$ be the set of all vectors of length n over $\mathbb{F}_q$. $\mathbb{F}_q^n$ is a vector space with dimension n over $\mathbb{F}_q$. The *projective space* $\mathcal{P}_q(n)$, is the set of all subspaces of $\mathbb{F}_q^n$, including $\{\mathbf{0}\}$ and $\mathbb{F}_q^n$. For a given integer k, $1 \leq k \leq n$, let $\mathcal{G}_q(n,k)$ denote the set of all k-dimensional subspaces of $\mathbb{F}_q^n$. $\mathcal{G}_q(n,k)$ is often referred to as Grassmannian. It is well known that

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \overset{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the *$q-$ary Gaussian coefficient* [115, pp. 325-332].

A *subspace code* $\mathbb{C}$ is a subset of $\mathcal{P}_q(n)$ and a *Grassmannian code* (known also as a *constant dimension code*) $\mathbb{C}$ is a subset of $\mathcal{G}_q(n,k)$. Clearly, the Grassmannian codes are subset of the subspace codes. In recent years there has been an increasing interest in subspace codes as a result of their application to error-correction in random network coding as was demonstrated by Koetter and Kschischang [70]. But, the interest in these codes has been also before this application, since Grassmannian codes are q-analogs of the well studied constant weight codes [23]. For example, the nonexistence of nontrivial perfect codes in the Grassmann scheme was proved in [27, 79]. The well-known concept of q-analogs replaces subsets by subspaces of a vector space over a finite field and their orders by the dimensions of the subspaces. In particular, the q-analog of a constant weight code in the Johnson space is a constant dimension code in the Grassmannian space. q-analogs of various combinatorial objects are well known [115, pp. 325-332]. Of special interest are q-analogs in extremal combinatoric as well as other well-known combinatorial problems, e.g. [14, 15, 28, 29, 53, 66]. The related techniques and results might be of usage in coding theory.

It turns out that the natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d_S(X,Y) \overset{\text{def}}{=} \dim X + \dim Y - 2\dim\big(X \cap Y\big) ,$$

for all $X, Y \in \mathcal{P}_q(n)$. This measure of distance is called the *subspace distance* and it is the q-analog of the Hamming distance in the Hamming space.

From the point of view of error-correction in random network coding it is better to use another measure of distance, called the *injection distance* given by

$$d_I(X,Y) = \max\{\dim(X), \dim(Y)\} - \dim(X \cap Y) .$$

The injection distance is the q-analog of the asymmetric distance between binary words [42, 47, 94]. Both, the subspace distance and the injection distance are metrics. When X and Y have the same dimension k, the subspace metric and the injection metric coincide. If $X,\ Y \in \mathcal{G}_q(n,k)$ then we can define their distance slightly different as follows,

$$d_G(X,Y) = k - \dim(X \cap Y) .$$

This measure of distance will be called the *Grassmannian distance*. The Grassmannian distance is the q-analog of the Johnson distance used for constant weight codes. It is equal to half of the subspace distance and it is equal exactly to the injection distance, i.e. $2d_G(X,Y) = d_S(X,Y) = 2d_I(X,Y)$.

The three measures of distance are metrics and they have related families of graphs $G(\mathcal{G}_q(n,k))$, $G(\mathcal{P}_q^S(n))$, and $G(\mathcal{P}_q^I(n))$, for the Grassmannian metric, the subspace metric, and the injection metric, respectively. The vertices of the graphs are the subspaces of $\mathcal{G}_q(n,k)$, $\mathcal{P}_q(n)$, and $\mathcal{P}_q(n)$, respectively. Two vertices X and Y are connected by an edge if the distance between X and Y is *one* in the Grassmannian metric, the subspace metric, and the injection metric, respectively.

This paper has three goals. The first one is to give a brief survey on the known results on q-analog problems in coding theory and related problems in block design. This will enable to put in one place all the relevant references in this area. The second goal of this paper is to suggest problems and questions for future research in this area and to motivate further research on the related topics. One hundred such questions and problems are presented. We remark that some problems might be contained in other problem, but the level of difficulty of such contained problems should be different. Other problems for future research will be understood from the text and the context. The third goal is to start some directions of solution in some of the given research problems. Each one of the sections which follows will be devoted to another topic in this area. In Section 2 we will discuss bounds on the size of Grassmannian codes. We will start to construct a table on the lower and upper bounds on the size of constant dimension codes in $\mathcal{P}_2(n)$ for $n \leq 7$. In Section 3 we will discuss the multilevel construction which is the most effective and simple way to construct very large Grassmannian codes or subspace codes with a given distance measure. The Grassmannian codes are usually larger than any other known codes with the same parameters. Bounds on the size of subspace codes with the subspace distance, are discussed in Section 4. We will present lower and upper bounds on the size of the codes in $\mathcal{P}_2(n)$ for $n \leq 7$. We will also present a new general bound and a related interesting problem, which is also interesting in the context of extremal combinatorics. In Section 5 we will discuss bounds on the size of subspace codes with the injection distance. A new interesting cyclic code which we present will raise some interesting questions. In Section 6 the existence question for q-analogs of Steiner systems which are one family of optimal Grassmannian codes, are discussed. We will present a new method which might lead for exclusion of parameters in which q-analog of Steiner systems can exist. In Section 7 we will discuss the concepts of spreads and partial spreads which are used in projective geometry, but they are also optimal Grassmannian codes. Section 8 will be devoted to rank-metric codes which are highly connected to Grassmannian codes and also to subspace codes. Encoding and decoding of subspace codes are discussed in Section 9. Designs over F_q, i.e. q-analogs of designs are considered in Section 10. In Section 11 we consider covering proplems in the projective space and the Grassmannian space. The asymptotic behavior of codes and designs in the projective space and the Grassmannian space is discussed in Section 12. Disjoint spreads are considered in Section 13. In Section 14 we discuss three more q-analog of coding problems. The first one is q-analog of Gray codes and in particular the q-analog of the the middle levels problem. The second problem is the existence question of complements in the projective space. The third problem is the existence question of linear codes in the projective space.

2 Constant Dimension Codes

A Grassmannian code is also called a constant dimension code since all the codewords have the same dimension. An $(n, \delta, k)_q$ code is a subset of $\mathcal{G}_q(n, k)$ with minimum Grassmannian distance δ. Let $\mathcal{A}_q(n, \delta, k)$ denote the maximum size of an $(n, \delta, k)_q$ code. Koetter and Kschischang [70], Etzion and Vardy [50] developed several upper bounds on $\mathcal{A}_q(n, \delta, k)$. For a subspace code $\mathbb{C}$ we define the *orthogonal complement* $\mathbb{C}^\perp$ as the code which consists of the dual subspaces of $\mathbb{C}$, i.e. $\mathbb{C}^\perp \overset{\text{def}}{=} \{X^\perp \ : \ X \in \mathbb{C}\}$. $\mathbb{C}$ and $\mathbb{C}^\perp$ have the same minimum distance (subspace, Grassmannian, or injection). Therefore, $\mathcal{A}_q(n, \delta, k) = \mathcal{A}_q(n, \delta, n-k)$ and hence in the sequel we will also consider only $(n, \delta, k)_q$ codes and only bounds on $\mathcal{A}_q(n, \delta, k)$ for which $2k \leq n$. The upper bounds on $\mathcal{A}_q(n, \delta, k)$ are usually the q-analog of the bounds in the Hamming scheme and the Johnson scheme. These include the sphere packing bound and the Singleton bound [70], the Johnson bounds [50, 117] from which the most important one is:

Theorem 1. $\mathcal{A}_q(n, \delta, k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \mathcal{A}_q(n-1, \delta, k-1) \right\rfloor$.

Theorem 1 can be iterated to obtain the iterated Johnson bound and the packing bound, which was proved earlier also in [116], where the context was linear authentication codes.

Theorem 2.

$$\mathcal{A}_q(n, \delta, k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n+\delta-k}-1}{q^\delta-1} \right\rfloor \cdots \right\rfloor \right\rfloor \leq \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} .$$

As for lower bounds on $\mathcal{A}_q(n, \delta, k)$, in [70] there is a construction, of codes based on linearlized polynomials, which yields the bound $\mathcal{A}_q(n, \delta, k) \geq q^{(n-k)(k-\delta+1)}$. The same bound was developed in [98] by using lifted rank-metric codes. In this context we define the rank distance and rank-metric codes which play an important role in the discussion on subspace codes. For two $k \times \ell$ matrices A and B over $\mathbb{F}_q$ the *rank distance* is defined by

$$d_R(A, B) \overset{\text{def}}{=} \text{rank}(A - B) .$$

A $[k \times \ell, \varrho, \delta]$ *rank-metric code* $\mathcal{C}$ is a linear code, whose codewords are $k \times \ell$ matrices over $\mathbb{F}_q$; they form a linear subspace with dimension ϱ of $\mathbb{F}_q^{k \times \ell}$, and for each two distinct codewords A and B we have that $d_R(A, B) \geq \delta$. For a $[k \times \ell, \varrho, \delta]$ rank-metric code $\mathcal{C}$ it was proved in [38, 54, 86] that

$$\varrho \leq \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\} . \tag{1}$$

This bound, called the Singleton bound for rank-metric codes, is attained for all feasible parameters. The codes which attain this bound are called *maximum rank distance* codes (or MRD codes in short).

Let A be a $k \times \ell$ matrix over $\mathbb{F}_q$ and let I_k be a $k \times k$ identity matrix. The matrix $[I_k \ A]$ can be viewed as a generator matrix of a k-dimensional subspace of $\mathbb{F}_q^{k+\ell}$, and it is called the *lifting* of A [98]. When all the codewords of a rank-metric code $\mathcal{C}$ are lifted to k-dimensional subspaces, the result is a constant dimension code $\mathbb{C}$. If $\mathcal{C}$ is an MRD code then $\mathbb{C}$ is called a *lifted MRD code* [98]. This code will be denoted by $\mathbb{C}^{\mathrm{MRD}}$. This code is not maximal and it can be extended by using a multilevel construction [48] as described in the next section. An upper bound on the size of a code which contains $\mathbb{C}^{\mathrm{MRD}}$ can be found in [49]. Codes based on linearlized polynomials, where each code contains the related code based on linearlized polynomial constructed in [70], were developed in [100]. But, these codes are smaller in size then the codes obtained by the multilevel construction.

Another family of Grassmannian codes are codes which admit a certain automorphism group. These kind of codes are discussed in [50, 71]. One of the most interesting family of such codes are the cyclic codes. Let $\mathbb{F}_{q^n}$ be a finite field with q^n elements, where q is a power of a prime number, and let α be a primitive element in $\mathbb{F}_{q^n}$. It is well-known that there is an isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$, where the *zero* elements are mapped into each other, and $\alpha^i \in \mathbb{F}_{q^n}$, $0 \leq i \leq q^n - 2$, is mapped into its q-ary n-tuple representation in $\mathbb{F}_q^n$, and vice versa. Using this mapping, a subspace of $\mathbb{F}_q^n$ is represented by the corresponding elements of $\mathbb{F}_{q^n}$. Let α be a primitive element of $\mathbb{F}_{q^n}$. We say that a code $\mathbb{C} \subseteq \mathcal{P}_q(n)$ is *cyclic* if it has the following property: whenever $\{\mathbf{0}, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_m}\}$ is a codeword of $\mathbb{C}$, so is its cyclic shift $\{\mathbf{0}, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_m+1}\}$. In other words, if we map each vector space $V \in \mathbb{C}$ into the corresponding binary characteristic vector $x_V = (x_0, x_1, \ldots, x_{2^n-2})$ given by

$$x_i = 1 \;\text{ if } \alpha^i \in V \qquad \text{and} \qquad x_i = 0 \;\text{ if } \alpha^i \notin V$$

then the set of all such characteristic vectors is closed under cyclic shifts. We note that the property of being cyclic does *not* depend on the choice of a primitive element α in $\mathbb{F}_{q^n}$.

Cyclic codes have a nice automorphism group. But, there are other automorphisms which can be forced on the code. One example is the use of the Frobenius mapping which was used for example in [18]. Some automorphisms of constant dimension codes were studied in [108]. Constructions for small dimensions might be attractive in this context. Interesting codes admitting some automorphisms were constructed in [22]. Some of these codes have an interesting combinatorial structure and some were found only by computer search. These were used to obtain lower bounds on $\mathcal{A}_2(n, 2, 3)$. Lower bounds on $\mathcal{A}_q(n, 2, 3)$ were also considered in [49]. Codes with subspaces of dimension 3 are of special interest mainly since the value of $\mathcal{A}_q(n, \delta, 2)$ is known for all parameters.

Another family of codes which was considered, even so the codes were not as large as in previous constructions, are the orbit codes [78, 109, 110, 114]. This family of codes might deserve further attention in the future. Another line of research for Grassmannain codes is based on Schubert calculus and Plücker coordinates. These were considered for example in [57, 111, 113] and their further research might lead to new interesting results. Lexicodes in the Grassmannian and their search were discussed in [96]. Codes which are able to correct also errors in coordinates (such as deletion or localized errors) are considered in [24, 101]. A question on the size of equidistant Grassmannian codes was asked in [50]. In an equidistant code, any two codewords have the same distance, which is clearly the minimum distance of the code. This problem is highly connected to problems in extremal combinatorics, e.g. [53, 61]. Some work in this direction was done lately in [62, 63, 64]. Finally, there are other related coding problems in the Grassmannian. For example, the intersection size of balls around codewords has some interesting applications [118], where the case for the intersection size two balls in the Grassmannian was considered.

We conclude this section with our first list of research problems.

Research problem 1. *Find a systematic construction for cyclic codes in* $\mathcal{G}_q(n,k)$.

Research problem 2. *Find new methods to construct large constant constant dimension codes which are not based on lifting of rank-metric codes.*

Research problem 3. *Can we derive some constraints to form a linear programming method to obtain new upper bounds on* $\mathcal{A}_q(n,\delta,k)$*?*

Research problem 4. *Find new general upper bounds on the size of Grassmannian codes.*

Research problem 5. *Find a general upper bound on the size of a Grassmannian code which contains* $\mathbb{C}^{MRD}$.

Research problem 6. *Improve the lower and upper bounds on* $\mathcal{A}_q(n,\delta,3)$ *for specific values of* n *and for large* n.

Research problem 7. *What is the size of the largest equidistant* $(n,\delta,k)_q$ *code?*

Research problem 8. *Find new applications for Grassmannian codes.*

Research problem 9. *Find the size of the intersection of more than two balls in the Grassmannian.*

Research problem 10. *Compile a table for the lower and upper bounds on* $\mathcal{A}_q(n,\delta,k)$ *for small values of* q, n, δ, *and* k.

We start with some tables related to Research problem 10. We consider the first few tables for $q=2$. Each table will be for a different value of $n \geq 4$. We omit the trivial cases where $k=1$ or $\delta=2$. We also consider only the cases where $k \leq n-k$ and ignore the cases where the size of the optimal code is one. By Theorem 8 we have that $\mathcal{A}_2(4,2,2)=5$; by Theorems 9 and 10 we have $\mathcal{A}_2(5,2,2)=9$. Hence, the first table is for $n=6$.

Bounds on $\mathcal{A}_2(6,\delta,k)$

δ	$k=3$	$k=2$
3	$^{a}9^{a}$	
2	$^{b}77-81^{c}$	$^{a}21^{a}$

Bounds on $\mathcal{A}_2(7,\delta,k)$

δ	$k=3$	$k=2$
3	$^{d}17^{d}$	
2	$^{e}329-381^{f}$	$^{g}31^{h}$

Bounds on $\mathcal{A}_2(8, \delta, k)$

δ	k = 4	3	2
4	${}^{a}17^{a}$		
3	${}^{i}257 - 289^{j}$	${}^{d}34^{d}$	
2	${}^{k}4797 - 6477^{f}$	${}^{e}1312 - 1493^{c}$	${}^{a}85^{a}$

- a - Theorem 8.
- b - [71].
- c - [50].
- d - [41].
- e - [22].
- f - Theorem 2.
- g - Theorem 10.
- h - Theorem 9.
- i - The Multilevel Construction with $\mathbb{C}^{\mathrm{MRD}}$.
- j - Theorem 1.
- k - [49].

Some of the specific values of $\mathcal{A}_q(n, \delta, k)$ can be of special interest. Some of these are discussed in Sections 6 and 7, but there are some other as well. For example, the value of $\mathcal{A}_2(2k, k-1, k)$, $k \geq 3$, is one such value. By Theorem 11 we have $\mathcal{A}_2(2k-1, k-1, k-1) = 2^k + 1$. Hence, by Theorem 1 we have $\mathcal{A}_2(2k, k-1, k) \leq \frac{2^{2k}-1}{2^k-1}(2^k+1) = (2^k+1)^2$. If there is a code which attains this bound then it should have a very interesting symmetry even so a code which attains the bound $\mathcal{A}_2(2k-1, k-1, k-1) = 2^k + 1$ does not have a symmetry. An interesting related question will be discussed in Section 4.

Research problem 11. *Is there some $k \geq 3$ for which $\mathcal{A}_2(2k, k-1, k) = (2^k+1)^2$? Does $\mathcal{A}_2(6, 2, 3) = 81$?*

Research problem 12. *Is there some $k \geq 4$ for which $\mathcal{A}_2(2k, k-1, k) \geq (2k+1)^2 - 2^{k-1}$? This bound will be of special interest in Section 4.*

3 The Multilevel Construction

The multilevel construction is a method for which the outcome is a code in $\mathcal{P}_q(n)$ which contains lifted rank-metric codes. The method can be used to construct Grassmannian codes, subspace codes with the subspace distance, and subspace codes with the injection distance. The construction is based on a new type of rank-metric codes, namely Ferrers diagram rank-metric codes. The description of the construction requires some methods to represent subspaces of $\mathcal{P}_q(n)$.

A k-dimensional subspace X of $\mathbb{F}_q^n$ can be represented by a $k \times n$ *generator matrix* whose rows form a basis for X. The basis of X is in *reduced row echelon form*, denoted by $E(X)$, if the following conditions are satisfied.

- The leading coefficient of a row is always to the right of the leading coefficient of the previous row.
- All leading coefficients are *ones*.
- Every leading coefficient is the only nonzero entry in its column.

Each k-dimensional subspace X of $\mathbb{F}_q^n$ has an *identifying vector* $v(X)$. $v(X)$ is a binary vector of length n and weight k, where the *ones* in $v(X)$ are in the positions (columns) where $E(X)$ has the leading *ones* (of the rows).

A *Ferrers diagram* represents partitions of positive integers as patterns of dots with the i-th row having the same number of dots as the i-th term in the partition [1, 102, 115]. A Ferrers diagram satisfies the following conditions.

- The number of dots in a row is at most the number of dots in the previous row.
- All the dots are shifted to the right of the diagram.

The *number of rows (columns)* of the Ferrers diagram $\mathcal{F}$ is the number of dots in the rightmost column (top row) of $\mathcal{F}$. If the number of rows in the Ferrers diagram is m and the number of columns is η we say that it is an $m \times \eta$ Ferrers diagram. If we read the Ferrers diagram by columns we get another partition of the same integer.

The *echelon Ferrers form* of a vector v of length n and weight k, $EF(v)$, is the $k \times n$ matrix in reduced row echelon form with leading entries (of rows) in the columns indexed by the nonzero entries of v and " $\bullet$ " in all entries which do not have terminals *zeroes* or *ones*. A " $\bullet$ " will be called in the sequel a *dot*. The dots of this matrix form the Ferrers diagram of $EF(v)$. If we substitute elements of $\mathbb{F}_q$ in the dots of $EF(v)$ we obtain a k-dimensional subspace X of $\mathcal{G}_q(n,k)$. $EF(v)$ will be called also the echelon Ferrers form of X.

Let v be a vector of length n and weight k and let $EF(v)$ be its echelon Ferrers form. Let $\mathcal{F}$ be the Ferrers diagram of $EF(v)$. $\mathcal{F}$ is an $m \times \eta$ Ferrers diagram, where $m \leq k$ and $\eta \leq n-k$. A code $\mathcal{C}$ is an $[\mathcal{F}, \varrho, \delta]$ *Ferrers diagram rank-metric code* if all codewords are $m \times \eta$ matrices in which all entries not in $\mathcal{F}$ are *zeroes*, it forms a rank-metric code with dimension ϱ, and minimum rank distance δ.

The Multilelvel Construction

First step: choose a binary code $\mathbf{C}$ of length n and minimum Hamming distance d, $2\delta-1 \leq d \leq 2\delta$. This code will be called the *skeleton code*.

The next three steps are performed for each codeword $c \in \mathbf{C}$.

Second step: construct the echelon Ferrers form $EF(c)$.

Third step: construct an $[\mathcal{F}, \varrho, \delta]$ Ferrers diagram rank-metric code $\mathcal{C}_{\mathcal{F}}$ for the Ferrers diagram $\mathcal{F}$ of $\text{EF}(c)$.

Fourth step: lift $\mathcal{C}_{\mathcal{F}}$ to an $(n, \delta, k)_q$ code $\mathbb{C}_c$, for which the echelon Ferrers form of $X \in \mathbb{C}_c$ is $\text{EF}(c)$.

Finally:

$$\mathbb{C} = \bigcup_{c \in \mathbf{C}} \mathbb{C}_c \ .$$

Theorem 3. *The size of the code $\mathbb{C}$ is $\sum_{c\in\mathbf{C}} |\mathbb{C}_c|$ and it has minimum subspace distance d.*

The code $\mathbb{C}$ obtained by the Multilevel Construction can be a Grassmannian code, a subspace code with the subspace distance, or a subspace code with the injection metric. If we want $\mathbb{C}$ to be a Grassmannian code then $\mathbf{C}$ must be a constant weight code in the Hamming scheme (or equivalently a code in the Johnson scheme). The other two options will be discussed in the next two sections. A comprehensive description and discussion on the Multilevel Construction can be found in [48]. Some improvements which enable to add more codewords for the final code can be found in [97, 112].

Research problem 13. *Find a method which combine the Multilevel Construction with more concepts to obtain larger codes.*

Research problem 14. *What is the best way to choose a skeleton code for the Multilevel Construction.*

4 Subspace Codes with the Subspace Distance

An $(n, d)_q^S$ code is a subspace code in $\mathcal{P}_q(n)$ with minimum subspace distance d. Let $\mathcal{A}_q^S(n, d)$ be the maximum number of codewords in an $(n, d)_q^S$ code. Recall that the Grassmannian distance is the q-analog of the Johnson distance and that the subspace distance is the q-analog of the Hamming distance. But, while the related Johnson graph, Grassmannian graph, and Hamming graph are distance regular, the related graph of $\mathcal{P}_q(n)$, $G(\mathcal{P}_q^S(n))$, is not distance regular. In fact, it is not regular since the sizes of the balls with radius one around a vertex depends on the dimension of the related subspace. This makes the task, of handling coding questions in $\mathcal{P}_q(n)$ in general and obtaining bounds on $\mathcal{A}_q^S(n, d)$ in particular, more difficult. Even so, classic lower bounds on $\mathcal{A}_q^S(n, d)$ such as the Gilbert-Varshamov bound were given in [50].

The Multilevel Construction can be applied to obtain subspace codes with the subspace distance, where the skeleton code is taken to be a binary code in the Hamming scheme. Subspace codes can be also cyclic codes. Hence, a method to construct cyclic subspace codes is one of the important tasks in this area. An example of a cyclic $(6, 3)_2^S$ code of size 85 was given in [50]. Construction of cyclic codes in $\mathcal{P}_q(n)$ is a method which should be further explored. A third method to construct subspace codes was presented in [48]. This is a puncturing method which is used to obtain codes with subspace distance $d-1$ from codes with subspace distance d. This method works as follows,

Let X be an ℓ-subspace of $\mathbb{F}_q^n$ such that the unity vector with an *one* in the i-th coordinate is not an element in X. The *puncturing* of the i-th coordinate of X, $\Delta_i(X)$, is defined as the ℓ-dimensional subspace of $\mathbb{F}_q^{n-1}$ obtained from X by deleting coordinate i from each vector in X. Let $\mathbb{C}$ be a code in $\mathcal{P}_q(n)$ and let Q be an $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$. Let $E(Q)$ be the $(n-1)\times n$ generator matrix of Q (in reduced row echelon form) and let τ be the position of the unique *zero* in $v(Q)$. Let $v \in \mathbb{F}_q^n$ be an element such that $v \notin Q$. We define the *punctured* code

$$\mathbb{C}'_{Q,v} = \mathbb{C}_Q \cup \mathbb{C}_{Q,v} ~,$$

where

$$\mathbb{C}_Q = \{\Delta_\tau(X) ~:~ X \in \mathbb{C},~ X \subseteq Q\})$$

and

$$\mathbb{C}_{Q,v} = \{\Delta_\tau(X \cap Q) ~:~ X \in \mathbb{C},~ v \in X\} ~.$$

This method is very useful and will usually produce codes which are larger than the codes generated by the Multilevel Construction when d is even and the resulting code has an odd subspace distance. It is also more effective in terms of good bounds when we start with a code of $\mathbb{F}_q^n$ for even n, in which a large $(n,\delta,\frac{n}{2})_q$ code is contained, and the resulting code contains subspaces of $\mathbb{F}_q^{n-1}$. Sometimes it would be better to start only with the related Grassmannian code $\mathbb{C}$ and to puncture $\mathbb{C}$. To the punctured code $\mathbb{C}'_{Q,v}$ codewords with other dimensions should be added. The right way, when and how to apply the puncturing method is a topic for future research.

The only reasonable known methods to obtain upper bounds on $\mathcal{A}_q^S(n,d)$ are various types of linear programming methods. The linear programming method suggested in [50] is different from the classic linear programming of Delsarte [36]. The classic linear programming does not yield any improvements, when applied for bounds on codes in $\mathcal{G}_q(n,k)$ or in $\mathcal{P}_q(n)$. A somehow stronger method is the semidefinite programming [90, 91] as suggested in [5] for the projective space. This method and the one in [50] yield all the best known upper bounds on $\mathcal{A}_q^S(n,d)$, when in most cases the semidefinite programming yields better bounds. The following list introduces a small list of the related research problems.

Research problem 15. *Find a counterpart Sphere packing bound on* $\mathcal{A}_q^S(n,d)$.

Research problem 16. *Find a q-analog for the well-known Plotkin bound on* $\mathcal{A}_q^S(n,d)$ *and analyze the related codes which attain the bound.*

Research problem 17. *Can additional constraints be added for the semidefinite programming to improve the upper bounds on* $\mathcal{A}_q^S(n,d)$*?*

Research problem 18. *Find a new method to construct large subspace codes with the subspace distance.*

Research problem 19. *Find a method to construct large cyclic codes in* $\mathcal{P}_q(n)$.

Research problem 20. *Compile a table with lower and upper bounds on $\mathcal{A}_q^S(n,d)$ for small q, n, and d.*

Let's consider Research problem 20 for $q=2$ and $4 \leq n \leq 7$. $\mathcal{A}_2^S(n,1) = |\mathcal{P}_q(n)|$ and $\mathcal{A}_2^S(n,2) = \Sigma_{\text{even } k} \begin{bmatrix} n \\ k \end{bmatrix}_2$, where $\mathcal{A}_2^S(n,2) = \frac{|\mathcal{P}_q(n)|}{2}$ for odd n. $\mathcal{A}_2^S(4,3) = \mathcal{A}_2^S(4,4) = 5$, where the lower bound is derived from a spread (see Section 7) and the upper bound is obtain using trivial analysis. It was proved that $\mathcal{A}_2^S(5,3) = 18$ in [50], by Theorem 4 we have $\mathcal{A}_2^S(5,4) = 9$, and it is easy to verify that $\mathcal{A}_2^S(5,5) = 2$. $\mathcal{A}_2^S(6,3) \leq 123$ as was proved in [50], where a lower bound of $\mathcal{A}_2^S(6,3) \geq 85$ was also given. The lower bound can be probably improved considerably by considering the 77 codewords of the $(6,2,3)_2$ code reported in [71] and adding to it subspaces with dimensions 2 and 4. The actual code size should be found by using a computer search. We leave it as we leave other basic computations which follow to the interested reader. $\mathcal{A}_2^S(6,4) = \mathcal{A}_2(6,2,3)$ and $\mathcal{A}_2^S(6,5) = \mathcal{A}_2^S(6,6) = \mathcal{A}_2(6,3,3) = 9$. $\mathcal{A}_2^S(7,3) \leq 776$ by using semidefinite programming as was proved in [5]. The lower bound $\mathcal{A}_2^S(7,3) \geq 584$ is obtained by puncturing the $(8,2,4)_2$ code of size 4797 [49] and adding to it the null space and $\mathbb{F}_2^7$. It is not difficult to verify based on previous results which were stated that $330 \leq \mathcal{A}_2^S(7,4) = \mathcal{A}_2(7,2,3)+1 \leq 382$. For the next two cases, $\mathcal{A}_2^S(7,5)$ and $\mathcal{A}_2^S(7,6)$ we will provide more detailed and general analysis.

Lemma 1. *If $\mathbb{C}$ is a $(2n+1,n,n+1)_2$ code of size $2^{n+1}+1$ then each one-dimensional subspace of $\mathbb{F}_2^{2n+1}$ is contained in one of its codewords.*

Proof. Assume the contrary, i.e. that no subspace of $\mathbb{C}$ contains a given vector $v \in \mathbb{F}_2^{2n+1}$. Let V be the one-dimensional subspace of $\mathbb{F}_2^n$ which contains v. Hence, $\mathbb{C}^\perp$ is an $(2n+1,n,n)_2$ code of size $2^{n+1}+1$ in which no codeword is contained in the $(2n)$-dimensional subspace $V^\perp$. Therefore, for each codeword $X \in \mathbb{C}^\perp$ we have $dim(X \cap V^\perp) = n-1$ and $|X \cap (\mathbb{F}_2^{2n+1} \setminus V^\perp)| = 2^{n-1}$. Clearly, for each two codewords $X,Y \in \mathbb{C}^\perp$ we have $\dim(X \cap Y)=0$. Therefore,

$$2^{2n} = |\mathbb{F}_2^{2n+1} \setminus V^\perp| \geq |\bigcup_{X \in \mathbb{C}^\perp} (X \cap V^\perp)| = \sum_{X \in \mathbb{C}^\perp} 2^{n-1} = 2^{2n} + 2^{n-1} ,$$

a contradiction. □

By Lemma 1, since $\mathcal{A}_2(2n+1,n,n+1) = \mathcal{A}_2(2n+1,n,n) = 2^{n+1}+1$ (see Theorem 11), and simple distance analysis (we also have to use the orthogonal complement code) we have

Theorem 4. $\mathcal{A}_2^S(2n+1,2n) = 2^{n+1}+1$.

Theorem 5. $2^{n+2}+1 \leq \mathcal{A}_2^S(2n+1,2n-1) \leq 2^{n+2}+2$.

Proof. The upper bound is implied by the same arguments as the ones for the proof of Theorem 4.

The lower bound is derived by puncturing a $(2n+2,n,n+1)_2$ $\mathbb{C}^{\text{MRD}}$ code $\mathbb{C}$ and adding one codeword to the punctured code.

The size of $\mathbb{C}$ is 2^{2n+2} and all the $2^{n+1}-1$ nonzero vectors of $\mathbb{F}_2^{2n+2}$ which start with $n+1$ *zeroes* are not contained in any codeword of $\mathbb{C}$. Each other nonzero vector of $\mathbb{F}_2^{2n+2}$ is contained in the same number of codeword (see [49]). Each codeword contains $2^{n+1}-1$ nonzero vectors of $\mathbb{F}_2^{2n+1}$. Hence, each of these $2^{2n+2}-2^{n+1}$ vectors is contained in $\frac{2^{2n+2}(2^{n+1}-1)}{2^{2n+2}-2^{n+1}} = 2^{n+1}$ codewords of $\mathbb{C}$.

Now, we compute the number of $(2n+1)$-dimensional subspaces of $\mathbb{F}_2^{2n+2}$ which contain a given $(n+1)$-dimensional subspace X of $\mathbb{F}_2^{n+1}$. The number of such $(2n+1)$-dimensional subspaces is

$$\frac{(2^{2n+2}-2^{n+1})(2^{2n+2}-2^{n+2})\ \cdots\ (2^{2n+2}-2^{2n})}{(2^{2n+1}-2^{n+1})(2^{2n+1}-2^{n+2})\ \cdots\ (2^{2n+1}-2^{2n})} = \frac{(2^{2n+2}-2^{n+1})2^{n-1}}{2^{2n+1}-2^{2n}} = 2^{n+1}-1 \ .$$

Hence, the number of $(2n+1)$-dimensional subspaces which do not contain all the $2^{n+1}-1$ nonzero vectors of $\mathbb{F}_2^{2n+2}$ which start with $n+1$ *zeroes* is $2^{2n+2}-1-(2^{n+1}-1) = 2^{2n+2}-2^{n+1}$.

Therefore, there exists at least one $(2n+1)$-dimensional subspace Q of $\mathbb{F}_2^{2n+2}$ which contains $\frac{2^{2n+2}(2^{n+1}-1)}{2^{2n+2}-2^{n+1}} = 2^{n+1}$ codewords ($(n+1)$-dimensional subspaces) of $\mathbb{C}$.

Thus, the punctured code $\mathbb{C}'_{Q,v}$, where v is any nonzero vector not in Q has size 2^{n+2}. To $\mathbb{C}'_{Q,v}$ we can add either any n-dimensional subspace which contains all the 2^n-1 vectors which start with n *zeroes* or any $(n+1)$-dimensional subspace which contains all these vectors, without damaging the minimum subspace distance.

Thus, $2^{n+2}+1 \leq \mathcal{A}_2^S(2n+1, 2n-1) \leq 2^{n+2}+2$. □

Note, that for any k for which $\mathcal{A}_2(2n+2, n, n+1) \geq (2n+3)^2 - 2^n$ (see Research problem 12) we will have $\mathcal{A}_2^S(2n+1, 2n-1) \leq 2^{n+2}+2$.

Research problem 21. *Find good bounds on the size of the $(n,d)_q^S$ code, $d = 2\delta+1$, which contains subspaces only with dimension k and $k-1$, where $\delta+2 \leq k \leq \lceil \frac{n}{2} \rceil$.*

Research problem 22. *Find good bounds on the size of the $(2k,d)_q^S$ code, d odd, which contains subspaces only with dimensions $k-1$, k, and $k+1$.*

Research problem 23. *Find a $(7,5)_2^S$ code with 34 codewords or prove that $\mathcal{A}_2^S(7,5) < 34$.*

Research problem 24. *Determine whether $\mathcal{A}_2^S(2n+1, 2n-1) = 2^{n+2}+1$ or $\mathcal{A}_2^S(2n+1, 2n-1) = 2^{n+2}+2$.*

Research problem 25. *What is the size of the largest equidistant $(n,d)_q^S$ code?*

Research problem 26. *Is the size of the largest equidistant $(n,d)_q^S$ code is greater by one from the size of the largest equidistant $(n, \lfloor \frac{n}{2}, d)_q$ code?*

Another question of interest is the existence question of perfect subspace codes with the subspace distance. It was proved in [50] that such codes do not exist. The Johnson space and the Grassmann space admit *diameter-perfect* codes [4]. All such diameter-perfect codes are optimal for their parameters. Unfortunately, the definition of diameter-perfect codes does not extend to the projective space $\mathcal{P}_q(n)$, since the size of a sphere in $\mathcal{P}_q(n)$ depends on its center.

Research problem 27. *Can one define another type of perfect codes in the projective space, so that certain optimal codes become "perfect" under this definition?*

5 The Injection Metric

An $(n,d)^I_q$ code is a subspace code in $\mathcal{P}_q(n)$ with minimum injection distance d. The injection distance is the one which is more useful, than the subspace distance, from a practical point of view [99]. Let $\mathcal{A}^I_q(n,d)$ denote the maximum number of codewords in an $(n,d)^I_q$ code. The injection distance is the q-analog of the asymmetric distance [68]. Also, the related graph $G(\mathcal{P}^I_q(n))$ is not distance regular which makes the analysis of some bounds more difficult as in the case of the subspace distance and the related graph $G(\mathcal{P}^S_q(n))$. Similarly to the Grassmannian codes and the subspace codes with the subspace distance, we can generate a large code for the injection metric by using the Multilevel Construction, where our skeleton code is a binary code with the asymmetric distance [68]. Instead of Hamming distance d for the skeleton code in the Multilevel Construction, we use asymmetric distance δ. Large asymmetric codes can be found for example in [42, 47, 94]. Puncturing is also useful to obtain good codes with the injection distance. But, puncturing constant dimension codes yields the same subspace codes with the injection distance as the ones with the subspace distance. Therefore, puncturing might be useful, to obtain good codes with the injection distance, when we start from a subspace code with the injection distance which is larger then the related code with the subspace distance. Another option is to puncture a Grassmannian code and to the punctured code, codewords with permitted dimensions (by the required injection distance) are added. We note that the permitted dimensions are more dense than in the case of a similar subspace code with the subspace distance. This will be further demonstrated and explained at the end of this section. Also, as in the case of the subspace distance, classic lower bounds such as the Gilbert-Varshamov bound were developed in [55, 68]. As for upper bounds, a linear programming was developed in [3], and in [5] there is a modification of the linear programming given in [50]. A semidefinite programming bound was also given in [5] and it was shown that the bounds obtained are very similar to those obtained by linear programming.

Research problem 28. *Find a counterpart Sphere packing bound on* $\mathcal{A}^I_q(n,d)$.

Research problem 29. *Compile a table with lower and upper bounds on* $\mathcal{A}^I_q(n,d)$ *for small* q*,* n*, and* d.

Research problem 30. *Find a new method to construct large subspace codes with the injection distance, which differ from the ones used for subspace codes with the subspace distance.*

Research problem 31. *Make a comprehensive comparison between the injection metric and the subspace metric, beyond consequences related to the asymmetric distance and the Hamming distance, respectively.*

For very small values of n related to a given injection distance d, the tables of Research problems 20 and 29 are very similar. For example, while $\mathcal{A}^S_2(4,4)=5$, the related bound for the injection distance is $\mathcal{A}^I_2(4,2)=7$ since we can add the null space and $\mathbb{F}^4_2$ to five subspaces of dimension two (since subspace codes with injection distance d can be denser than their related subspace codes with subspace distance $2d-1$). But, in some cases, we can find much larger codes with nice structure for the injection distance. As an example we consider $n=6$

and injection distance 2. Let α be a root of x^6+x+1, and use this primitive polynomial to generate $\mathbb{F}_{64}$. Consider the code $\mathbb{C}$ in $\mathcal{P}_2(6)$ which consists of all the cyclic shifts of

$$\{\mathbf{0}, \alpha^0, \alpha^{21}, \alpha^{42}\}\ ,$$

$$\{\mathbf{0}, \alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\}\ ,$$

and

$$\{\mathbf{0}, \alpha^0, \alpha^1, \alpha^6, \alpha^8, \alpha^{18}, \alpha^{21}, \alpha^{22}, \alpha^{27}, \alpha^{29}, \alpha^{39}, \alpha^{42}, \alpha^{43}, \alpha^{48}, \alpha^{50}, \alpha^{60}\}\ .$$

To the 105 subspaces obtained in this process we add the null space and $\mathbb{F}_2^6$ to obtain a cyclic $(6,2)_2^I$ code of size 107 which implies that $\mathcal{A}_2^I(6,2) \geq 107$, which is much better than what we can obtain for a related $(6,3)_2^S$ code. The upper bounds in both cases are very similar, since by linear programming we have $\mathcal{A}_2^I(6,2) \leq 125$, while $\mathcal{A}_2^S(6,2) \leq 123$.

Research problem 32. *Find good bounds on the size of a* $(2k,d)_q^I$ *code, d odd, which contains subspaces only with dimensions* $k-1$, k, *and* $k+1$. *Compare the bounds with the related bounds on the large size of a* $(2k,2d-1)_q^S$ *code.*

Research problem 33. *Find large cyclic subspace codes with the injection distance.*

6 q-Analog of Steiner Systems

A *Steiner system* $S(t,k,n)$ is a collection S of k-subsets from an n-set $\mathcal{N}$ such that each t-subset of $\mathcal{N}$ is contained in exactly one element of S. Steiner systems were subject to an extensive research in combinatorial designs [33]. A Steiner system is also equivalent to an optimal constant weight codes in the Hamming scheme.

Cameron [25, 26] and Delsarte [37] have extended the notions of block design and Steiner systems to vector spaces. A *Steiner structure* (*q-Steiner system*) $\mathbb{S}_q(t,k,n)$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n,k)$ (called *blocks*) such that each element from $\mathcal{G}_q(n,t)$ is contained in exactly one block of $\mathbb{S}$. A Steiner structure $\mathbb{S}_q(t,k,n)$ is a constant dimension code which attains the bound of $\mathcal{A}_q(n,k-t+1,k)$. Similarly, to Steiner systems, simple necessary divisibility conditions for the existence of a given Steiner structure are developed [93].

Theorem 6. *If a Steiner structure* $\mathbb{S}_q(t,k,n)$ *exists then for each* i, $1 \leq i \leq t-1$, *a Steiner structure* $\mathbb{S}_q(t-i,k-i,n-i)$ *exists.*

Corollary 1. *If a Steiner structure* $\mathbb{S}_q(t,k,n)$ *exists then for all* $0 \leq i \leq t-1$.

$$\frac{\begin{bmatrix} n-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q}$$

must be integers.

Steiner structures and Steiner systems are highly related. In [52, 93] there are some constructions of Steiner systems derived from Steiner structures. Further research on Steiner structures seems to be fascinating, but also extremely difficult. We list some interesting, but probably very difficult research problems.

Research problem 34. *Let $\mathbb{S}$ be a Steiner structure $\mathbb{S}_q(t,k,n)$. Find new sets of parameters $t' < k' < n'$ for which there exists a Steiner system $S(t',k',n')$ derived from $\mathbb{S}$.*

Research problem 35. *Are there more Steiner structures embedded in a Steiner structure $\mathbb{S}_q(t,k,n)$, except from the ones implied by Theorem 6.*

Until recently, the only known Steiner structures $\mathbb{S}_q(t,k,n)$ were either trivial or for $t=1$, where such structures exist if and only if k divides n. These are called spreads and they will be discussed in the next section. Thomas [107] showed that certain kind of Steiner structures $\mathbb{S}_2(2,3,7)$ cannot exist. Metsch [81] conjectured that nontrivial Steiner structures with $t \geq 2$ do not exist. Steiner structures appear also in connection of diameter perfect codes in the Grassmann scheme. It was proved in [4] that the only diameter perfect codes in the Grassamnn scheme are the q-Steiner systems. The following theorem given in [52] has given more indication that finding Steiner structures with $t \geq 2$ would be a very difficult task.

Theorem 7. *If there exists a Steiner structure $\mathbb{S}_2(2,k,n)$ then there exists a Steiner system $S(3,2^k,2^n)$.*

As a consequence of Theorem 7, we have that if there exists a Steiner structure $\mathbb{S}_2(2,3,7)$ then there exists a Steiner system $S(3,8,128)$. The existence of a Steiner system $S(3,8,128)$ is an open problem, which might strengthen the conjecture that a Steiner structure $\mathbb{S}_2(2,3,7)$ does not exist.

Recently, the first Steiner structure $\mathbb{S}_q(t,k,n)$ with $t \geq 2$ was found. This is a Steiner structure $\mathbb{S}_2(2,3,13)$ which have a large automorphism group [18]. We will describe this group in terms of two mappings and an equivalence relation defined on k-dimensional subspaces. Let α be a primitive element in $\mathbb{F}_{q^n}$ and define the following two mappings

The *Frobenius mapping* Υ_ℓ, $0 \leq \ell \leq n-1$, $\Upsilon_\ell : \mathbb{F}_{q^n} \setminus \{0\} \longrightarrow \mathbb{F}_{q^n} \setminus \{0\}$ is defined by $\Upsilon_\ell(x) \stackrel{\text{def}}{=} x^{q^\ell}$ for each $x \in \mathbb{F}_{q^n} \setminus \{0\}$.

The *cyclic shift mapping* Φ_j, $0 \leq j \leq q^n-2$, $\Phi_j : \mathbb{F}_{q^n} \setminus \{0\} \longrightarrow \mathbb{F}_{q^n} \setminus \{0\}$ is defined by $\Phi_j(\alpha^i) \stackrel{\text{def}}{=} \alpha^{i+j}$, for each $0 \leq i \leq q^n-2$.

The two types of mappings Υ_ℓ and Φ_j can be applied on a subset or a subspace, by applying the mapping on each element of the subset or the subspace, respectively. Formally, given two integers $0 \leq \ell \leq n-1$ and $0 \leq j \leq q^n-2$,

$$\Upsilon_\ell\{x_1,x_2,\ldots,x_r\} \stackrel{\text{def}}{=} \{\Upsilon_\ell(x_1),\Upsilon_\ell(x_2),\ldots,\Upsilon_\ell(x_r)\}\ ,$$

$$\Phi_j\{x_1,x_2,\ldots,x_r\} \stackrel{\text{def}}{=} \{\Phi_j(x_1),\Phi_j(x_2),\ldots,\Phi_j(x_r)\}.$$

We define the following equivalence relation $\tilde{E}$ on the subspaces of $\mathcal{G}_q(n,k)$.

$$(X,Y) \in \tilde{E} \quad \text{if} \quad \text{there exist two integers, } \ell_1,\ j_1, \text{ such that } Y = \Phi_{j_1}(\Upsilon_{\ell_1}(X))\ .$$

In [18] Steiner structures $\mathbb{S}_q(t,k,n)$, in which a k-dimensional subspace X is contained in the system if all its equivalence class, under the equivalence relation $\tilde{E}$, is contained in the structure, are considered. Such structures can be described with a relatively small number of representatives. The Steiner structure $\mathbb{S}_2(2,3,13)$ constructed in [18] was constructed in this way and only 15 representatives describe the whole system. The knowledge on q-Steiner systems is very small and there are many more research problems for future research. As we noted before, these problems are probably extremely difficult. The next few problems to consider are as follows.

Research problem 36. *Prove or disprove that a q-Steiner system* $\mathbb{S}_2(2,3,7)$ *exists.*

Research problem 37. *Construct more q-Steiner systems* $\mathbb{S}_2(2,3,n)$*, where* $n \equiv 1 \ (mod\ 6)$ *is a prime.*

Research problem 38. *By using the equivalence relation* $\tilde{E}$*, develop the theory and find an example of a q-Steiner system* $\mathbb{S}_2(2,4,n)$ *for some n; and* $\mathbb{S}_q(2,3,n)$ *for some* $q > 2$ *and some n.*

Research problem 39. *Find parameters for which the necessary conditions for the existence conditions for a q-Steiner systems* $\mathbb{S}_q(t,k,n)$ *are satisfied, but the systems do not exist.*

Research problem 40. *Find new necessary conditions for the existence of q-Steiner systems.*

We conclude this section with a method that can lead for the construction of a q-Steiner system $\mathbb{S}_2(2,3,7)$ or to a proof for its nonexistence. This method will be called the *projections method* and it is described for a general q-Steiner system $\mathbb{S}_q(t,k,n)$.

We start by assuming that $\mathbb{S}$ is a q-Steiner system $\mathbb{S}_q(t,k,n)$. Each r-dimensional subspace Z of $\mathbb{F}_q^n$ will be represented by an $n \times \frac{q^r-1}{r-1}$ matrix whose columns represent the nonzero vectors contained in Z, where the leading nonzero element in a vector is an *one*. For a given ρ, $1 \leq \rho \leq n$, we construct a system $\mathbb{S}_\rho$, which consists of the projections of the first ρ rows of each subspace of $\mathbb{S}$. Each $\rho \times \frac{q^r-1}{r-1}$ matrix formed in this way represents an ℓ-dimensional subspace of $\mathbb{F}_q^\rho$ for some ℓ, $0 \leq \ell \leq \min\{\rho, k\}$. Similarly, the projection of the first ρ rows in a t-dimensional subspace is an ℓ-dimensional subspace of $\mathbb{F}_q^\rho$ for some ℓ, $0 \leq \ell \leq \min\{\rho, t\}$. For each i, $0 \leq i \leq \min\{\rho, k\}$, we have $\begin{bmatrix} \rho \\ i \end{bmatrix}_q$ variables. A variable a_Y for each i-dimensional subspace Y of $\mathbb{F}_q^\rho$. The value of a variable is the number of times the related i-dimensional subspace appears in the system $\mathbb{S}_\rho$. For each i, $0 \leq i \leq \min\{\rho, t\}$, we generate $\begin{bmatrix} \rho \\ i \end{bmatrix}_q$ equations. An equation for each i-dimensional subspace of $\mathbb{F}_q^\rho$. Let X be such an i-dimensional subspace of $\mathbb{F}_q^\rho$. Let δ_X the number of distinct ways to complete X into a t-dimensional subspace of $\mathbb{F}_q^n$. Let $\Gamma_{X,Y}$ be the number of times that X is contained in an ℓ-dimensional subspace Y of $\mathbb{F}_q^\rho$ such that $i \leq \ell$ (taking into account that X is completed into a t-dimensional subspace and Y is completed into a k-dimensional subspace). For each such i-dimensional subspace X we generate the equation

$$\delta_X = \sum_{\substack{Y \in \mathbb{F}_q^\rho \\ \dim X \leq \dim Y}} \Gamma_{X,Y} a_Y \ .$$

If the system of equations does not have a nonnegative integer solution then a q-Steiner system $\mathbb{S}_q(t,k,n)$ does not exist.

Example 1. *Let $n = 7$, $k = 3$, $t = 2$, and $\rho = 2$. Let a_0 be the variable for the null space X_0. Let a_1, a_2, a_3 be the variable for the one-dimensional subspaces of $\mathbb{F}_2^2$, $X_1 = \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\}$, $X_2 = \left\{ \begin{array}{c} 1 \\ 0 \end{array} \right\}$, $X_3 = \left\{ \begin{array}{c} 1 \\ 1 \end{array} \right\}$, respectively. Let a_4 be the variable for the two-dimensional subspace $X_4 = \left\{ \begin{array}{ccc} 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \right\}$ of $\mathbb{F}_2^2$. One can easily verify that $\delta_{X_0} = \begin{bmatrix} 5 \\ 2 \end{bmatrix}_2 = 155$, $\delta_{X_1} = \delta_{X_2} = \delta_{X_3} = \binom{32}{2} = 496$, and $\delta_{X_4} = 32^2 = 1024$. Note, that $\begin{bmatrix} 5 \\ 2 \end{bmatrix}_2 + 3\binom{32}{2} + 32^2 = \begin{bmatrix} 7 \\ 2 \end{bmatrix}_2 = 2667$. Now, let $Y_i = X_i$ for $0 \leq i \leq 4$. We now have $\Gamma_{X_0,Y_0} = 7$, $\Gamma_{X_0,Y_i} = 1$, $\Gamma_{X_i,Y_i} = 6$, $\Gamma_{X_i,Y_4} = 1$, for $i = 1, 2, 3$, and $\Gamma_{X_4,Y_4} = 4$. For any other i and j we have $\Gamma_{X_i,Y_j} = 0$.*

Therefore, we have the following 5 equations:

1. $155 = 7a_0 + a_1 + a_2 + a_3$.
2. $496 = 6a_1 + a_4$.
3. $496 = 6a_2 + a_4$.
4. $496 = 6a_3 + a_4$.
5. $1024 = 4a_4$.

This system of equations has exactly one solution, $a_0 = 5$, $a_1 = a_2 = a_3 = 40$, and $a_4 = 256$.

If $n = 7$, $k = 3$, $t = 2$, and $\rho = 4$ then there are $\begin{bmatrix} 4 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 + \begin{bmatrix} 4 \\ 3 \end{bmatrix}_2 = 66$ variables and $\begin{bmatrix} 4 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 51$ equations. From the 16 variables which represents the null space and the 15 one-dimensional subspaces exactly one variable should be equal *one*. If we set one of these 16 variables to *one* then there is a unique solution to the set of equations. For example, if the variable which represents the null subspace is equal to *one* then each variable out of the 35 variables which represent the 35 two-dimensional subspaces is equal to 4 and each variable out of the 15 variables which represent the 15 three-dimensional subspaces is equal to 16.

If $n = 7$, $k = 3$, $t = 2$, and $\rho = 5$ then there are $\begin{bmatrix} 5 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 5 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 5 \\ 2 \end{bmatrix}_2 + \begin{bmatrix} 5 \\ 3 \end{bmatrix}_2 = 342$ variables and $\begin{bmatrix} 5 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 5 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 5 \\ 2 \end{bmatrix}_2 = 187$ equations. A computer program found a large number of solutions to these equations.

If $n = 7$, $k = 3$, $t = 2$, and $\rho = 6$ then there are $\begin{bmatrix} 6 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 6 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 6 \\ 2 \end{bmatrix}_2 + \begin{bmatrix} 6 \\ 3 \end{bmatrix}_2 = 2110$ variables and $\begin{bmatrix} 6 \\ 0 \end{bmatrix}_2 + \begin{bmatrix} 6 \\ 1 \end{bmatrix}_2 + \begin{bmatrix} 6 \\ 2 \end{bmatrix}_2 = 715$ equations. We were not able to handle the system of equations, but this system might be the key to settle the existence question of a q-Steiner system $\mathbb{S}_2(2, 3, 7)$.

Research problem 41. *Finish the projections method to settle the existence problem of a q-Steiner system $\mathbb{S}_2(2, 3, 7)$.*

Research problem 42. *Find more necessary conditions for the existence of a q-Steiner system $\mathbb{S}_q(t, k, n)$ by using the projections method.*

Research problem 43. *Apply the projections method on various parameters for q-Steiner systems $\mathbb{S}_q(t, k, n)$ either to exclude the existence of some systems or to find more insight on the existence question.*

7 Spreads and Partial Spreads

Two subspaces X, Y of $\mathcal{P}_q(n)$ are called *disjoint* if their intersection is the null space, i.e. $X \cap Y = \{\mathbf{0}\}$. A *spread* $\mathbb{S}$ in $\mathcal{G}_q(n,k)$ is a set of pairwise disjoint subspaces of $\mathcal{G}_q(n,k)$ in which each one-dimensional subspace of $\mathcal{P}_q(n)$ is a subspace of exactly one element of $\mathbb{S}$. A *partial spread* $\mathbb{S}$ in $\mathcal{G}_q(n,k)$ is a set of pairwise disjoint subspaces of $\mathcal{G}_q(n,k)$ in which each one-dimensional subspace of $\mathcal{P}_q(n)$ is a subspacce of at most one element of $\mathbb{S}$. A spread in the Grassmannian $\mathcal{G}_q(n,k)$ is clearly a constant dimension code with $\frac{q^n-1}{q^k-1}$ codewords and minimum Grassmannian distance k. It attains the bound on $\mathcal{A}_q(n,k,k)$ and it is also a q-Steiner system $\mathbb{S}_q(1,k,n)$. Any $(n,k,k)_q$ code is a *partial spread.* A spread is also a well-known and important concept in projective geometry. The projective geometry $\mathrm{PG}(n,q)$ consists of $\frac{q^{n+1}-1}{q-1}$ points and $\frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}$ lines. The points are represented by a set of nonzero elements from $\mathbb{F}_q^{n+1}$, of maximum size, in which each two elements are linearly independent. Each element x of these $\frac{q^{n+1}-1}{q-1}$ elements represents $q-1$ elements of $\mathbb{F}_q^{n+1}$ which are the multiples of x by the nonzero elements of $\mathbb{F}_q$. A line in $\mathrm{PG}(n,q)$ consists of $q+1$ points. Given two distinct points x and y, there is exactly one line which contains these two points. This line contains x and y and the $q-1$ points of the form $\gamma x+y$, where $\gamma \in \mathbb{F}_q \setminus \{0\}$. A point is a 0-subspace in $\mathrm{PG}(n,q)$, a line is a 1-subspace in $\mathrm{PG}(n,q)$, and a k-subspace is constructed by taking a $(k-1)$-subspace Y and a point x not on Y and all points that are constructed by a linear combination of x with any set of points from Y. We note that there is a difference of one in the definition between the dimensions of subspaces in projective geometry and subspaces in the projective space (or the Grassmannian). In the sequel, we will continue to use the notation used for the Grassmannian. A k-spread in $\mathrm{PG}(n,q)$ is a set of pairwise disjoint k-subspaces of $\mathrm{PG}(n,q)$ for which any point of $\mathrm{PG}(n,q)$ is contained in exactly one k-subspace. Such a k-spread is a spread in $\mathcal{G}_q(n+1,k+1)$. Spreads and partial spreads are basic concepts which were very well studied in projective geometry. We will not go into all the details, except for some concepts related to spreads which will be discussed in the sections which follow. We already mentioned that a spread in $\mathcal{G}_q(n,k)$, where k divides n is a Steiner structure $\mathbb{S}_q(1,k,n)$. The value of $\mathcal{A}_q(n,k,k)$ is of a very special interest. This value has a special interest since $(n,k,k)_q$ codes have applications as byte-correcting codes [43, 65]. Decoding of such constant dimension codes was considered in [58, 77]

The known upper and lower bounds on $\mathcal{A}_q(n,k,k)$ are summarized in the following theorems. The first three well-known theorems can be found in [50].

Theorem 8. *If k divides n then $\mathcal{A}_q(n,k,k)=\frac{q^n-1}{q^k-1}$.*

Theorem 9. $\mathcal{A}_q(n,k,k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor -1$ *if $n \not\equiv 0 \pmod{k}$.*

Theorem 10. *Let $n \equiv r \pmod{k}$. Then, for all q, we have*

$$\mathcal{A}_q(n,k,k) \geq \frac{q^n-q^k(q^r-1)-1}{q^k-1}$$

We note that one method to obtain the lower bound of Theorem 10 is to apply the Multilevel Construction. The next theorem was proved in [65] for $q=2$ and for any other q in [9].

Theorem 11. *If* $n \equiv 1 \pmod{k}$ *then* $\mathcal{A}_q(n,k,k) = \frac{q^n-q}{q^k-1} - q + 1 = \sum_{i=1}^{\frac{n-1}{k}-1} q^{ik+1} + 1$.

The bound of Theorem 11 is attained with $\mathbb{C}^{\text{MRD}}$ to which one subspace is added. By Theorems 8 and 11, the value of $\mathcal{A}_q(n,2,2)$ is known for all values of q and n. Theorem 11 was extended for the case where $q=2$ and $k=3$ in [41] as follows.

Theorem 12. *If* $n \equiv c \pmod{3}$ *then* $\mathcal{A}_2(n,3,3) = \frac{2^n-2^c}{7} - c$.

The upper bound implied by Theorem 11 was improved for some cases in [39] in which a transformation, of partial spreads into orthogonal arrays of strength two, is considered.

Theorem 13. *If* $n = k\ell + c$ *with* $0 < c < k$, *then* $\mathcal{A}_q(n,k,k) \leq \sum_{i=0}^{\ell-1} q^{ik+c} - \Omega - 1$, *where* $2\Omega = \sqrt{1 + 4q^k(q^k - q^c)} - (2q^k - 2q^c + 1)$.

Research problem 44. *Improve the lower bound on* $\mathcal{A}_q(n,k,k)$ *given in Theorem 10.*

Research problem 45. *Characterize the cases in which the lower bound on* $\mathcal{A}_q(n,k,k)$ *given in Theorem 10 is the exact value of* $\mathcal{A}_q(n,k,k)$.

Research problem 46. *Improve the upper bound on* $\mathcal{A}_q(n,k,k)$ *given in Theorem 13.*

Research problem 47. *Find more parameters for which we can give the exact value of* $\mathcal{A}_q(n,k,k)$ *as given in Theorem 11.*

Research problem 48. *Find the value of* $\mathcal{A}_q(n,3,3)$ *for all* q *and* n.

Research problem 49. *Find the value of* $\mathcal{A}_2(n,4,4)$ *for a new infinite family of values of* n.

8 Rank-Metric Codes

Ferrers diagram rank-metric codes are the key for large codes based on the Multilevel Construction. Therefore, it is important (at least theoretically) to find large Ferrers diagram rank-metric codes. Let $\dim(\mathcal{F},\delta)$ be the the largest possible dimension of an $[\mathcal{F},\varrho,\delta]$ code. The following theorem for the upper bound on the size of such codes was proved in [48].

Theorem 14. *For a given* i, $0 \leq i \leq \delta - 1$, *if* ν_i *is the number of dots in a Ferrers diagram* $\mathcal{F}$, *which are not contained in the first* i *rows and are not contained in the rightmost* $\delta - 1 - i$ *columns then* $\min_i\{\nu_i\}$ *is an upper bound of* $\dim(\mathcal{F},\delta)$.

The bound of Theorem 14 is attained trivially for $\delta = 1$ and also attained for $\delta = 2$ and for some sporadic parameters [48]. Therefore, the most important questions in this context are as follows.

Research problem 50. *Find more parameters for which the bound of Theorem 14 is attained.*

Research problem 51. *Prove that the bound of Theorem 14 is attained for all sets of parameters,* $\mathcal{F}$, q, *and* δ; *or disprove this claim.*

Rank-metric codes can raise some more interesting questions, but usually these questions do not have a direct application or any relation for subspace codes. However, a specific type of rank-metric codes, namely *constant rank codes* have an important direct application to constant dimension codes. These codes were considered in [56]. A constant rank code is a rank-metric code in which all codewords have the same rank.

Let $\mathcal{A}_q^R(m,n,d,r)$ be the maximum number of codewords in a constant rank code with constant rank r and minimum rank distance d over $\mathbb{F}_q^{n\times m}$. The following two theorems [56] are the most relevant ones in the context of optimal constant dimension codes.

Theorem 15. *For all q, $2k \leq n \leq m$ and $1 \leq \delta \leq r$ we have $\mathcal{A}_q(n,\delta,r) = \mathcal{A}_q^R(m,n,\delta+r,r)$ if either $\delta = r$ or $m \geq (n-r)(r-\delta+1)+r+1$.*

Theorem 16.

1. $\mathcal{A}_q^R(m,n,r+1,r) = \begin{bmatrix} n \\ r \end{bmatrix}_q$.

2. $\mathcal{A}_q^R(n,m,2r,r) = \mathcal{A}_q(n,r,r)$ *(the largest partial spread).*

Research problem 52. *Find constructions for constant rank codes which are not derived from the known constructions of constant dimension codes.*

Research problem 53. *Continue to develop the theory of constant rank codes beyond the results given in [56].*

Research problem 54. *Find the exact value of $\mathcal{A}_q^R(n,m,\delta+r,r)$ for $2 \leq \delta < r$, where $m \geq (n-r)(r-\delta+1)+r+1$.*

Research problem 55. *Develop the theory for $\mathcal{A}_q^R(n,m,\delta+r,r)$ for $2 \leq \delta < r$, where $m < (n-r)(r-\delta+1)+r+1$.*

9 Decoding of Subspace Codes

Error-correcting codes over any channel are constructed for the purpose of correcting errors caused during the transmission of the information on the channel. Therefore, from a theoretical point of view one might be interested in the size of the largest possible code. But, from a practical point of view when a code is constructed, we are more interested in its decoding (but not neglecting the requirement for a large code). For some of the first constructions mentioned earlier the authors gave decoding algorithms, e.g. [48, 58, 70, 77, 98, 100]. All these decoding algorithms are based on maximum likelihood decoding. Most of these decoding algorithms are for Grassmannian codes, but some can be adopted for subspace codes with either the subspace distance or the injection distance. Quite naturally also list-decoding algorithms were developed for Grassmannian codes (constructed either by linearlized polynomials or as lifted rank-metric codes), e.g [2, 59, 60, 73, 74, 75, 76, 85, 111]. Also, this direction of research has many problems for future research.

Research problem 56. *Suggest new classes of large Grassmannian codes, subspace codes (with the subspace distance or the injection distance) with efficient decoding algorithms.*

Research problem 57. *Design a list-decoding algorithm for codes which are not subcodes of either linearlized polynomial codes or lifted rank-metric codes.*

Research problem 58. *Find good lower and upper bounds on the size of Grassmannian codes for list-decoding when the size of the list is a small constant.*

Research problem 59. *Find good lower and upper bounds on the size of subspace codes (not necessarily Grassmannian) for list-decoding when the size of the list is a small constant.*

The subspace codes constructed by the various construction methods are not linear and therefore we should have an encoding algorithm from the list of information words into the list of codewords. If the code consists for example from one lifted MRD code then the encoding is trivial by using the encoding of the related rank-metric code. If the code is constructed by the Multilevel Construction then the encoding is slightly more complicated and it was described in [69]. Finally, encoding of all the Grassmannian space was described in [80, 95].

Research problem 60. *Find better encoding algorithms for subspace codes, the Grassmannian $\mathcal{G}_q(n,k)$, or the projective space $\mathcal{P}_q(n)$.*

10 Designs over GF(q)

q-analog of Steiner systems are one type of q-analog of designs, also called designs over $\mathbb{F}_q$. As was mentioned before, the notion of t-design have been extended to vector spaces by Cameron [25, 26] and Delsarte [37] in the early 1970s.

A $t-(n,k,\lambda)_q$ design is a collection $\mathbb{B}$ of k-dimensional subspaces (called *blocks*) from $\mathcal{G}_q(n,k)$ such that each t-dimensional subspace of $\mathcal{G}_q(n,t)$ is contained in exactly λ blocks of $\mathbb{B}$. If $\mathbb{B}$ contains all the k-dimensional subspaces of $\mathcal{G}_q(n,k)$ then the design is said to be trivial.

Thomas [106] was the first to find nontrivial t-design over $\mathbb{F}_q$, which are not spreads. The work of Thomas has motivated other research work to explore this topic and more t-designs over $\mathbb{F}_q$ were found [20, 67, 84, 104, 105, 107].

Another type of design over $\mathbb{F}_q$ which was defined is the *subspace transversal design* [49]. It is not a direct q-analog of a transversal design as will be explained in the sequel.

Let $\mathbb{V}^{(n,k)}$ be the set of nonzero vectors of $\mathbb{F}_q^n$ whose first k entries form a nonzero vector. For a given $X \in \mathcal{G}_q(k,1)$, let $\mathbb{V}_X^{(n,k)}$ denote the set nonzero vectors in $\mathbb{F}_q^n$ whose first k entries form any given nonzero vector of X. Let $\mathbb{V}_{\mathbf{0}}^{(n,k)}$ denote a maximal set of $\frac{q^{n-k}-1}{q-1}$ nonzero vectors in $\mathbb{F}_q^n$ whose first k entries are *zeroes*, for which any two vectors in the set are linearly independent. Let $\mathbb{V}_{\mathbf{0}}$ denote the k-dimensional subspace spanned by $\mathbb{V}_{\mathbf{0}}^{(n,k)}$.

A *subspace transversal design* of groupsize q^{n-k}, block dimension k, and *strength* t, denoted by $\text{STD}_q(t,k,n-k)$, is a triple $(\mathbb{V},\mathbb{G},\mathbb{B})$, where $\mathbb{V}$ is a set of points, $\mathbb{G}$ is a set of groups, and $\mathbb{B}$ is a set of blocks. These three sets must satisfy the following five properties:

1. $\mathbb{V}$ is a set of size $\frac{q^k-1}{q-1}q^{n-k}$ (the *points*). $\bigcup_{X\in\mathcal{G}_q(k,1)}\mathbb{V}_X^{(n,k)}$ is used as the set of points $\mathbb{V}$.

2. $\mathbb{G}$ is a partition of $\mathbb{V}$ into $\frac{q^k-1}{q-1}$ classes of size q^{n-k} (the *groups*); the groups which are used are defined by $\mathbb{V}_X^{(n,k)}$, $X \in \mathcal{G}_q(k,1)$.

3. $\mathbb{B}$ is a collection of k-dimensional subspaces of $\mathbb{F}_q^n$ which contain nonzero vectors only from $\mathbb{V}^{(n,k)}$ (the *blocks*);

4. each block meets each group in exactly one point;

5. every t-dimensional subspace (with points from $\mathbb{V}$) which meets each group in at most one point is contained in exactly one block.

This is not a direct q-analog of a transversal design since the elements of $\mathbb{V}_{\mathbf{0}}^{(n,k)}$ don't participate in any block of the design. It was proved in [49] that the codewords of an $(n,\delta,k)_q$ $\mathbb{C}^{\text{MRD}}$ form the blocks of a $\text{STD}_q(k-\delta+1,k,n-k)$. It was also shown in [49] how to use the properties of subspace transversal design to obtain better bounds on $\mathcal{A}_q(n,\delta,k)$ with codes which contains $\mathbb{C}^{\text{MRD}}$. These properties were also used to construct q-covering designs [44] and parallelisms [45] and they probably can be used for constructions of other related structures.

Research problem 61. *Find new $t-(n,k,\lambda)_q$ designs with new parameters.*

Research problem 62. *Find q-analogs for other known types of block designs for which an application for a construction of subspace codes can be given.*

Research problem 63. *Find q-analogs for other types of combinatorial designs, such as Latin squares, orthogonal arrays, etc.*

Research problem 64. *Prove that for each $1 < t < k$ and each q there exists an integer $n_0 > k$ such that for each $n > n_0$ a nontrivial $t-(n,k,\lambda)_q$ design exists.*

Recently, another type of q-analog for designs was considered. This is a large set of a $t-(n,k,\lambda)_q$ design. A *large set* of a design $\mathcal{S}$ is a partition of the space into disjoint copies of $\mathcal{S}$. Hence, a large set of $t-(n,k,\lambda)_q$ designs is a partition of $\mathcal{G}_q(n,k)$ into disjoint copies of $t-(n,k,\lambda)_q$ designs. Parallelism in projective geometry is a large set and this topic will be discussed separately in Section 13. Braun, Kohnert, Östergård, and Wassermann [21] presented a large set of $2-(8,3,21)_2$ designs. This large set consists of three disjoint $2-(8,3,21)_2$ designs.

Research problem 65. *Find more large sets of $t-(n,k,\lambda)_q$ designs.*

11 q-Covering Designs

A *q-covering design* $\mathbb{C}_q(n,k,r)$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,r)$ is contained in at least one element of $\mathbb{S}$. Let $\mathcal{C}_q(n,k,r)$ denote the minimum number of subspaces in a q-covering design $\mathbb{C}_q(n,k,r)$.

q-covering designs were considered first in the context of projective geometry. A set $\mathbb{T}$ of t-subspaces in $\text{PG}(n,q)$ such that each s-subspace contains at least one element of $\mathbb{T}$ is called a *blocking set*. Such a design is a q-analog of the well-known *Turán design* [34, 35]. The dual subspaces of the subspaces in a blocking set form a q-covering design $\mathbb{C}_q(n+1, n-t, n-s)$. Blocking sets were considered for example in [82, 83]. We note that blocking sets have also some different definitions (and maybe more popular definitions which define other structures which are not q-coverings).

Similarly, to the case of error-correcting codes in the projective space (which are q-packing designs) there are some basic bounds on the size of a q-covering design. The first one is the q-analog Schönheim bound [92] which was given in [52].

Theorem 17. $\mathcal{C}_q(n,k,r) \geq \left\lceil \frac{q^n-1}{q^k-1} \mathcal{C}_q(n-1,k-1,r-1) \right\rceil$.

The basic covering bound is given in the following theorem [52].

Theorem 18. $\mathcal{C}_q(n,k,r) \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}_q}{\begin{bmatrix} k \\ r \end{bmatrix}_q}$ *with equality holds if and only if a Steiner structure* $\mathbb{S}_q(r,k,n)$ *exists.*

As in the case of the q-analog Johnson bound (Theorem 2) also the q-analog Schönheim bound can be iterated.

Theorem 19.

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

Another lower bound given in [52] is a q-analog of a theorem given by de Caen in [34, 35].

Theorem 20. $\mathcal{C}_q(n,k,k-1) \geq \frac{(q^k-1)(q-1)}{(q^{n-k}-1)^2} \begin{bmatrix} n \\ k+1 \end{bmatrix}_q$.

The following two theorems given for example in [52] are also simple to obtain.

Theorem 21. *If* $1 \leq k \leq n$, *then* $\mathcal{C}_q(n,k,1) = \left\lceil \frac{q^n-1}{q^k-1} \right\rceil$.

Theorem 22. *If* $1 \leq r \leq n-1$, *then* $\mathcal{C}_q(n,n-1,r) = \frac{q^{r+1}-1}{q-1}$.

Theorem 22 was proved before in the context of projective geometry by Bose and Burton in [16]. Another lower bound was given in [40] by considering sets of lines in $\mathrm{PG}(2s,q)$ contained in s-subspaces.

Theorem 23. $\mathcal{C}_q(2s+1, 2s-1, s) \geq \frac{q^{2s+2}-q^2}{q^2-1} + \frac{q^{s+1}-1}{q-1}$ *for every integer* $s \geq 2$.

Metsch [82] also gave a construction for a set of lines in $\mathrm{PG}(2s+x-1,q)$, for every $1 \leq x \leq s$, contained in s-subspaces, which yields the following theorem:

Theorem 24. *For any given integers* $q \geq 2$, $1 \leq x \leq s$ *we have* $\mathcal{C}_q(2s+x, 2s+x-2, s+x-1) \leq \frac{q^{2s+2x}-q^{2x}}{q^2-1} + \frac{q^x-1}{q-1} \cdot \frac{q^{s+x}-q^{x-1}}{q-1}$.

Finally, also Theorem 21 was proved in terms of projective geometry. In projective geometry, the quantity $\mathcal{C}_q(n+1,k+1,1)$, is the minimum number of k-subspaces in $\text{PG}(n,q)$ such that each point of $\text{PG}(n,q)$ is contained in at least one of these subspaces. The solution obtained in Theorem 21 was obtained before by Beutelspacher [10]. The proofs for all these results and related results in projective geometry were also given by Metsch in [82].

The most basic upper bound, given by construction, on the size of a q-covering design was proved in [52].

Theorem 25. $\mathcal{C}_q(n,k,r) \leq q^{n-k}\mathcal{C}_q(n-1,k-1,r-1)+\mathcal{C}_q(n-1,k,r)$.

Normal spreads [72], also known as geometric spreads [12], are used to prove the following values of $\mathcal{C}_q(n,k,r)$ [13].

Theorem 26. $\mathcal{C}_q(vm+\delta, vm-m+\delta, v-1) = \frac{q^{vm}-1}{q^m-1}$ *for all* $v \geq 2$, $m \geq 2$, *and* $\delta \geq 0$.

The next theorem given in [52] is used infinitely many times once an exact bound for some given parameters is known.

Theorem 27. $\mathcal{C}_q(n+1,k+1,r) \leq \mathcal{C}_q(n,k,r)$.

Theorem 27 implies a very interesting property on the behavior of optimal q-design coverings.

Corollary 2. *For any given* $r > 0$ *and* $\delta > 0$ *there exists a constant* $c_{q,\delta,r}$ *and an integer* n_0 *such that for each* $n > n_0$, $\mathcal{C}_q(n,n-\delta,r) = c_{q,\delta,r}$.

The usage of lifted MRD codes as subspace transversal designs made it possible to obtain some interesting bounds on $\mathcal{C}_2(n,k,2)$ and $\mathcal{C}_2(n,k,3)$ [44].

Research problem 66. *Find new techniques to construct q-covering designs for $q = 2$.*

Research problem 67. *Find new techniques to obtain new lower bounds on $\mathcal{C}_2(n,k,r)$.*

Research problem 68. *Improve the bounds on $\mathcal{C}_2(n,k,r)$ for $n \leq 10$ (tables for the known bounds are given in [44]).*

Research problem 69. *Find new parameters for which the exact value of $\mathcal{C}_2(n,k,r)$ can be obtained.*

Research problem 70. *Develop new techniques to construct q-covering designs for $q > 2$ and generate related tables for the bounds on $\mathcal{C}_q(n,k,r)$ for small q, e.g. $q = 3$, 4, and 5.*

Research problem 71. *Make use of subspace transversal designs to obtain new bounds on $\mathcal{C}_q(n,k,r)$ for $q > 2$ or for $q = 2$ and $r > 3$.*

Another type of codes which can be considered are covering codes in the projective space which are the q-analog for covering codes in the Hamming scheme. A code $\mathbb{C}$ is a q-covering code with covering radius R in $\mathcal{P}_q(n)$ if $\mathbb{C}$ consists of subspaces from $\mathcal{P}_q(q)$ and for each subspace $X \in \mathcal{P}_q(n)$ there exists a subspace $Y \in \mathbb{C}$ such that $d_S(X,Y) \leq R$. Let $\mathcal{C}_q(n,R)$ be the minimum size of a q-covering code with radius R in $\mathcal{P}_q(n)$. To develop the theory of q-covering codes in $\mathcal{P}_q(n)$ we can consider the following problems.

Research problem 72. *Develop some basic lower bounds on $\mathcal{C}_q(n, R)$.*

Research problem 73. *Develop constructions to obtain upper bounds on $\mathcal{C}_q(n, R)$.*

Research problem 74. *Compile a table with lower and upper bounds on $\mathcal{C}_q(n, R)$ for small values of q and n.*

Some work in this direction was done in [55]. The bounds on $\mathcal{C}_q(n, k, r)$ can play an important role in this direction (to obtain bounds on $\mathcal{C}_q(n, R)$) in the same way that the bounds on $\mathcal{A}_q(n, \delta, k)$ play an important role when the bounds on $\mathcal{A}_q^S(n, d)$ are considered. These covering questions can be considered similarly for the injection distance instead of the subspace distance. Covering codes can be considered also for the injection distance [55]. But, q-covering codes are mainly interesting from a theoretical point of view. From combinatorial perspective the subspace distance is more interesting than the injection distance and hence covering codes with the injection distance might attract less attention.

12 Asymptotic Behavior

One important topic to consider is the asymptotic behavior of $\mathcal{A}_q(n, d, k)$, $\mathcal{A}_q^S(n, d)$, $\mathcal{A}_q^I(n, d)$, $\mathcal{C}_q(n, k, r)$, and $\mathcal{C}_q(n, R)$. A family of Grassmannian codes $\mathbb{C}_n$, of subspaces from $\mathcal{G}_q(n, k)$ with minimum Grassmannian distance δ, is called *asymptotically optimal* if $\frac{|\mathbb{C}_n|}{\mathcal{A}_q(n,\delta,k)} \rightarrow 1$ as $n \rightarrow \infty$. The quantity $\frac{|\mathbb{C}_n|}{\mathcal{A}_q(n,\delta,k)}$ as $n \rightarrow \infty$ is called the *density* of the code. Similarly, we define asymptotically optimal subspace codes with either the subspace distance or the injection distance, and q-covering designs. Density for the other types of codes is also defined similarly. It is quite obvious that there could be many cases in which we are not able to know whether the codes are asymptotically optimal since we don't know the magnitude of the optimal codes. Therefore, in the context of the asymptotic behavior we are concerned with the following three problems:

1. What is the size of an asymptotically optimal code?
2. What are the lower bounds on the density of the known codes (upper bounds for covering codes and designs)?
3. Constructions of asymptotically optimal codes.

Of course, we are mostly interested for an answer to the third problem since constructions of asymptotically optimal codes also determine the size of asymptotically optimal codes and produces codes with density one.

Research problem 75. *Find constructions for families of asymptotically optimal Grassmannian codes.*

Research problem 76. *Find constructions for families of asymptotically optimal q-covering designs.*

But, when a construction of such asymptotically optimal codes is not available we would like to consider solutions for the the other two problems.

Blackburn and Etzion [13] consider the asymptotic behavior of Grassmannian codes and q-covering designs. They first presented a connection between the size of an optimal Grassmannian code and the size of an optimal q-covering design.

Theorem 28. *We have that*

$$\mathcal{C}_q(n,k,k-\delta) \leq \mathcal{A}_q(n,\delta+1,k) + \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{A}_q(n,\delta+1,k)$$

and

$$\mathcal{A}_q(n,\delta+1,k) \geq \mathcal{C}_q(n,k,k-\delta) + \begin{bmatrix} n \\ k-\delta \end{bmatrix}_q - \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q \mathcal{C}_q(n,k,k-\delta).$$

Let $A(n) \sim B(n)$ means that $\lim_{n\to\infty} A(n)/B(n) = 1$. By considering hypergraphs, probabilistic arguments, and Theorem 28 we have the following two theorems [13].

Theorem 29. *Let q, k and δ be fixed integers, with $0 \leq \delta \leq k$ and such that q is a prime power. Then*

$$\mathcal{A}_q(n,\delta+1,k) \sim \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q} \tag{2}$$

as $n \to \infty$.

Theorem 30. *Let q, k and δ be fixed integers, with $0 \leq \delta \leq k$ and such that q is a prime power. Then*

$$\mathcal{C}_q(n,k,k-\delta) \sim \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}$$

as $n \to \infty$.

For specific values, asymptotically optimal Grassmannian codes and q-covering designs were mentioned in the previous sections. But, the following problems remained unsolved for most parameters.

Research problem 77. *Extend the range for which the size of asymptotically optimal Grassmannian codes can be shown.*

Research problem 78. *What is the asymptotic behavior of $\mathcal{A}_q^S(n,d)$ and $\mathcal{A}_q^I(n,d)$?*

Research problem 79. *What is the asymptotic behavior of $\mathcal{A}_q(n,\delta,k)$ when δ or k are not fixed?*

Research problem 80. *What is the asymptotic behavior of $\mathcal{C}_q(n,k,r)$ when k or r are not fixed?*

Research problem 81. *What is the asymptotic behavior of $\mathcal{C}_q(n,R)$?*

When we cannot construct asymptotically optimal codes we are interested in dense Grassmannian codes and sparse q-covering designs. Koetter and Kschischang [70] proved that the density of $\mathbb{C}^{\mathrm{MRD}}$ codes is at least $\frac{1}{4}$. Thus, this class of codes is good enough for any practical purpose. The lower bounds on the density were considerably improved with better constructions and improved upper bounds on the size of the codes. An analysis of the lower bounds on the densities is given in [49], where it was shown that the density is at least $\frac{3}{5}$. Some work in this direction for q-covering designs was done in [44]. But, there is a lot of ground for further research in this direction.

Research problem 82. *Show a general bound of considerably more than $\frac{3}{5}$ for the density of Grassmannian codes.*

Research problem 83. *Produce a comprehensive analysis of the densities for Grassmannian codes and q-covering designs.*

13 Parallelism

A k-spread is called a parallel class as it partition the set of all the points of $\mathrm{PG}(n,q)$. A k-parallelism in $\mathrm{PG}(n,q)$ is a partition of the k-subspaces of $\mathrm{PG}(n,q)$ into pairwise disjoint k-spreads. Hence, a parallelism is also a type of a large set as mentioned in Section 10. Some 1-parallelisms of $\mathrm{PG}(n,q)$ are known for many years. For $q=2$ and odd n there is an 1-parallelism in $\mathrm{PG}(n,2)$. Such a parallelism was found in the context of Preparata codes and it is known that many such parallelisms exist [6, 7, 119]. For any other power of a prime q, if $n=2^i-1$, $i\geq 2$, then an 1-parallelism was shown in [8]. In the last forty years no new parameters for 1-parallelisms were shown until recently, when an 1-parallelism in PG(5,3) was proved to exist in [51]. A k-parallelism for $k>1$ was not known until a 2-parallelism in $\mathrm{PG}(5,2)$ was shown in [87].

Clearly, such parallelisms can be described in terms of spreads in the Grassmannian. As it seems to be extremely difficult, we consider two problems which are generalizations of the parallelism problem. The first one is to consider what is the maximum number of pairwise disjoint k-spreads that exist in $\mathrm{PG}(n,q)$? Beutelspacher [11] has proved that if n is odd then there exist $q^{2\lfloor \log n\rfloor}+\cdots+q+1$ pairwise disjoint 1-spreads in $\mathrm{PG}(n,q)$. It is proved in [45] that two disjoint k-spreads exist in $\mathrm{PG}(n,q)$ and $2^{k+1}-1$ pairwise disjoint spreads exist in $\mathrm{PG}(n,2)$.

For the second problem, we will define a *partial Grassmannian* $\mathcal{G}_q(n_1,n_2,k)$, $n_1>n_2\geq k$, as the set of all k-dimensional subspaces from the space $\mathbb{F}_q^{n_1}$ which are not contained in a given n_2-dimensional subspace U of $\mathbb{F}_q^{n_1}$. It can be readily verified that $\mathbb{V}^{(n,k)}$ is a partial Grassmannian $\mathcal{G}_q(n,n-k,k)$, where $\mathbb{V}_0^{(n,k)}$ is the $(n-k)$-dimensional subspace U. A spread in $\mathcal{G}_q(n_1,n_2,k)$ is a set $\mathbb{S}$ of pairwise disjoint k-dimensional subspaces from $\mathcal{G}_q(n_1,n_2,k)$ such that each nonzero element of $\mathbb{F}_q^{n_1}\setminus U$ is contained in exactly one element of $\mathbb{S}$. A parallelism of $\mathcal{G}_q(n_1,n_2,k)$ is a set of pairwise disjoint spreads in $\mathcal{G}_q(n_1,n_2,k)$ such that each k-dimensional subspace of $\mathcal{G}_q(n_1,n_2,k)$ is contained in exactly one of the spreads. Beutelspacher [11] proved that if $k=2$ then such a parallelism exists if $n_2\geq 2$, $n_1-n_2=2^i$, for all $i\geq 1$ and any $q>2$. If $k=2$ and $q=2$ then such a parallelism exists if and only if $n_2\geq 3$ and n_1-n_2 is even. Etzion [45] proved that if $k=n_1-n_2$ then there exists a parallelism in $\mathcal{G}_q(n_1,n_2,k)$

Research problem 84. *For any $q > 2$ and $k \geq 1$, improve the lower bounds on the number of pairwise disjoint k-spreads in PG(n, q).*

Research problem 85. *For $q = 2$ and any $k > 1$, improve the lower bounds on the number of pairwise disjoint k-spreads in PG(n, q).*

Research problem 86. *Find nontrivial necessary conditions for the existence of a parallelism in $\mathcal{G}_q(n_1, n_2, k)$.*

Research problem 87. *Find new parameters for which there exists a parallelism in $\mathcal{G}_q(n_1, n_2, k)$.*

Research problem 88. *For a power of a prime $q > 2$, find new parameters for which there exists an 1-parallelism in PG(n, q).*

Research problem 89. *For $k > 1$ and any power of a prime q, starting with $q = 2$, find new parameters for which there exists a k-parallelism in PG(n, q).*

Research problem 90. *For $k > 1$, find an infinite family of k-parallelisms in PG(n, q).*

14 Other Problems in Coding Theory

There are many other interesting problems in connections to coding theory which can be defined on the projective space and the Grassmannian. We will consider three topics: Gray codes, self-complements codes, and linear codes.

14.1 Gray Codes

Gray codes have many applications and they are defined on variety of objects [88]. A Gray code in $\mathcal{P}_q(n)$ or $\mathcal{G}_q(n,k)$ is a path in the related graphs $G(\mathcal{P}_q^S(n))$ and $G(\mathcal{G}_q(n,k))$, respectively. In $G(\mathcal{P}_q^S(n))$ the vertices represent the subspaces of $\mathbb{F}_q^n$. Two vertices X and Y are connected by an undirected edge if $d_S(X,Y) = 1$. In $G(\mathcal{G}_q(n,k))$ the vertices represent the k-dimensional subspaces of $\mathbb{F}_q^n$. Two vertices X and Y are connected by an undirected edge if $d_S(X,Y) = 2$ ($d_G(X,Y) = 1$). The goal is to find the longest path and if possible a path which contains all the vertices in the graph, i.e. it will be a Hamiltonian path. Moreover, it is also desired that the path will be a cycle. One can easily verify that in $\mathcal{P}_q(n)$ there is no Hamiltonian path if n is even since the number of vertices with even dimension is greater than the number of vertices with odd dimension. Therefore, the four obvious research problems can be stated as follows.

Research problem 91. *Is there a Hamiltonian cycle in $G(\mathcal{P}_q^S(n))$, n odd?*

Research problem 92. *What is the the length of the longest path in $G(\mathcal{P}_q^S(n))$?*

Research problem 93. *What is the the length of the longest cycle in $G(\mathcal{P}_q^S(n))$?*

Research problem 94. *Is there a Hamiltonian cycle in $G(\mathcal{G}_q(n,k))$?*

Research problem 95. *What is the the length of the longest path in $G(\mathcal{G}_q(n,k))$?*

We note that the graph $G(\mathcal{P}_q^I(n))$ is not of interest for this problem as it lacks the natural combinatorial structure as the other two graphs.

Another interesting problem in this context is the q-analog of the middle levels problem which is a well-known unsolved problem for the Hamming graph [89]. The q-analog problems are presented as follows.

Research problem 96. *Is there a cycle in $G(\mathcal{P}_q^S(2k+1))$ which contains all the k-dimensional subspaces and all the $(k+1)$-dimensional subspaces?*

Research problem 97. *What is the length of the longest path in $G(\mathcal{P}_q^S(2k+1))$ which contains only k-dimensional subspaces and $(k+1)$-dimensional subspaces?*

In [46] it is shown that for any given q and $k = 1$ or $k = 2$ there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(2k+1)$. The method is using cyclic shifts of subspaces in a modification of a similar method which is making use of necklaces in the Hamming graph.

14.2 Complements

Complements of binary codewords and binary codes are used as a tool in various aspects of coding theory. The q-analog was considered in [19]. Various related problems concerning complements of subspaces over $\mathbb{F}_q$ were considered before, e. g. [30, 31, 32].

Definition 1. *Let $\mathcal{U}$ be a subset of $\mathcal{P}_q(n)$ and let $\mathcal{U}_k := \mathcal{U} \cap \mathcal{G}_q(n,k)$. We say that a function $f : \mathcal{U} \to \mathcal{U}$ is a* complement *on $\mathcal{U}$ (and denote $\overline{X} = f(X)$ for all $X \in \mathcal{U}$) if f has the following properties:*

P1. *$X \cap \overline{X} = \{\mathbf{0}\}$ and $X + \overline{X} = \mathbb{F}_q^n$, i.e. $X \oplus \overline{X} = \mathbb{F}_q^n$ for all $X \in \mathcal{U}$.*

P2. *f establishes a bijection between $\mathcal{U}_k$ and $\mathcal{U}_{n-k}$ for all k, $0 \leq k \leq n$.*

P3. *$f(f(X)) = X$ for all $X \in \mathcal{U}$.*

P4. *$d_S(\overline{X}, \overline{Y}) = d_S(X, Y)$ for all $X, Y \in \mathcal{U}$.*

The existence problems of complements in $\mathcal{P}_q(n)$ was considered in [19]. Some of the results are based on representation of subspaces by lattices [17]. The main open problem which remains unsolved in this discussion is our next open problem.

Research problem 98. *Prove that the largest subset of $\mathcal{P}_q(n)$ on which a complement can be defined is the set $\mathcal{V}_q(n) = \{X \in \mathcal{P}_q(n) : X \cap X^\perp = \{\mathbf{0}\}\}$; or disprove this claim.*

A closed-form expression for $|\mathcal{V}_q(n)|$ was given by Sendrier [103]. Using the results of [103], it can be shown that the size of $\mathcal{V}_q(n)$ is *proportional* to $|\mathcal{P}_q(n)|$, specifically:

$$\lim_{n\to\infty} \frac{|\mathcal{V}_q(n)|}{|\mathcal{P}_q(n)|} = \prod_{i=1}^{\infty} \frac{1}{1+q^{-i}} \; .$$

The limit converge to $0.4194\ldots$ when $q = 2$, $0.639\ldots$ when $q = 3$, $0.7375\ldots$ when $q = 4$, and $0.9961\ldots$ when $q = 256$.

14.3 Linear Codes

Linear codes are one of the basic concepts in coding theory. In [19] there is a comprehensive discussion of q-analog of linear codes in the projective space.

Definition 2. *Let $\mathcal{U}$ be a subset of $\mathcal{P}_2(n)$ with $\{\mathbf{0}\} \in \mathcal{U}$. We say that $\mathcal{U}$ is a* linear code *in $\mathcal{P}_2(n)$ if there exists a function $\boxplus : \mathcal{U} \times \mathcal{U} \rightarrow \mathcal{U}$ such that $(\mathcal{U}, \boxplus)$ is an abelian group with the following properties: the identity element is $\{\mathbf{0}\}$, and the inverse of every group element $X \in \mathcal{U}$ is X itself. The function $\boxplus$ is* isometric*, namely:*

$$d_S(X \boxplus Y_1, X \boxplus Y_2) = d_S(Y_1, Y_2) \quad \textit{for all} \quad X, Y_1, Y_2 \in \mathcal{U} \ .$$

The discussion in [19] yields a linear code of size 2^n in $\mathcal{P}_2(n)$ and two intriguing questions remained open.

Research problem 99. *Prove that the size of the largest linear code in $\mathcal{P}_2(n)$ is 2^n or show a linear code in $\mathcal{P}_2(n)$ of size 2^{n+1}.*

Research problem 100. *Given a linear code $\mathbb{C}$, in $\mathcal{P}_2(n)$, which contains $\mathbb{F}_2^n$ as a codeword, prove or disprove that the number of codewords with dimension k in $\mathbb{C}$ is at most $\binom{n}{k}$.*

Acknowledgments

I am grateful to Alexander Vardy for many discussions on the topics mentioned in this paper. This survey was motivated by COST Action IC1104 "Random Network Coding and Designs over GF(q)". It should be acknowledged that this action has made it possible to bring together many researchers in related areas for common discussions and new joint research on problems related to this paper.

References

[1] G. E. Andrews and K. Eriksson, *Integer Partitions*, Cambridge University Press, 2004.

[2] R. Agarwal, *Combinatorial lower bound for list decoding of codes on finite field Grassmannian,* in proc. of *ISIT 2011*, pp. 2293–2297.

[3] R. Ahlswede and H. K. Aydinian, *On error control codes for random network coding,* in proc. of *NetCod 2009*, pp. 68–73.

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

[5] C. Bachoc, A. Passuello, and F. Vallentin, *Bounds for projective codes from semidefinite programming, Advances of Mathematics in Communications*, 7 (2013), 127–145.

[6] R. D. Baker, *Partitioning the planes $AG_{2m}(2)$ into 2-designs*, *Discrete Math.*, 15 (1976), 205–211.

[7] R. D. Baker, J. H. van Lint, nd R. M. Wilson, *On the Preparata and Goethals codes*, *IEEE Trans. Inform. Theory*, 29 (1983), 342–345.

[8] A. Beutelspacher, *On parallelisms in finite projective spaces, Geometriae Dedicata,* 3 (1974), 35–40.

[9] A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs, Math. Zeit.,* 145 (1975), 211–229.

[10] A. Beutelspacher, *On t-covers in finite projective spaces, Geometriae Dedicata,* 12 (1979), 10–16.

[11] A. Beutelspacher, *Partial parallelisms in finite projective spaces*, *Geometriae Dedicata*, 36 (1990), 273–278.

[12] A. Beutelspacher and J. Ueberberg, *A characteristic property of geometric t-spreads in finite projective spaces, Europ. J. Comb.,* 12 (1991), 277–281.

[13] S. Blackburn and T. Etzion, *The Asymptotic Behavior of Grassmannian Codes*, *IEEE Trans. Inform. Theory*, 58 (2012), 6605–6609.

[14] A. Blokhuis, A. E. Brouwer, and T. Szőnyi, *On the chromatic number of q-Kneser graphs*, *Designs, Codes, and Cryptography,* 65 (2012), 187–197.

[15] A. Blokhuis, A. E. Brouwer, T. Szőnyi, and Zs. Weiner, *On q-analogues and stability theorems, J. Geometry,* 101 (2011), 31–50.

[16] R. C. Bose and R.C. Burton, *A characterization of flat spaces in finite geometry and the uniqueness of the Hamming and the MacDonald codes, Journal Combinatorial Theory,* 1 (1966), 96–104.

[17] M. Braun, *On lattices, binary codes, and network codes*, *Advances of Mathematics in Communications*, 5 (2011), 225–232.

[18] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann *Existence of q-Analogs of Steiner Systems, arxiv.org/abs/1304.1462*, April 2013.

[19] M. Braun, T. Etzion, and A. Vardy, *Linearity and Complements in Projective Space, Linear Algebra and its Applications,* 438 (2013), 57–70.

[20] M. Braun, A. Kerber, and R. Laue, *Systematic construction of q-analogs of* $t-(v,k,\lambda)$*-designs, Designs, Codes, and Cryptography,* 34 (2005), 55–70.

[21] M. Braun, A. Kohnert, P. R. J. Östergård, and A. Wassermann *Large Sets of t-Designs over Finite Fields, arxiv.org/abs/1305.1455*, May 2013.

[22] M. Braun and J. Reichelt, *q-Analog of packing designs, arxiv.org/abs/1212.4614*, December 2012.

[23] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, *A new table of constant weight codes*, *IEEE Trans. on Inform. Theory*, 36 (1990), 1334–1380.

[24] N. Cai, *A new table of constant weight codes, IEEE Trans. on Inform. Theory*, 59 (2013), 3282–3294.

[25] P. Cameron, Generalisation of Fisher's inequality to fields with more than one element, in T.P. McDonough and V.C. Mavron, Eds., *Combinatorics*, London Math. Soc. Lecture Note Ser. 13 Cambridge Univ. Press, Cambridge, 1974, pp. 9–13.

[26] P. Cameron, *Locally symmetric designs*, *Geometriae Dedicata,* 3 (1974), 65–76.

[27] L. Chihara, *On the zeros of the Askey-Wilson polynomials, with applications to coding theory, SIAM J. Math. Anal.,* 18 (1987), 191–207.

[28] A. Chowdhury C. Godsil, and G. Royle, *Colourings lines in projective space, Journal of Combinatorial Theory, Series A,* 113 (2006), 39–52.

[29] A. Chowdhury and B. Patkós, *Shadows and intersections in vector spaces, Journal of Combinatorial Theory, Series A,* 117 (2010), 1095–1106.

[30] W. E. Clark, *Matching subspaces with complements in finite vector spaces, Bull. Inst. Combin. Appl.,* 6 (1992), 33–38.

[31] W. E. Clark and B. Shekhtman, *Covering by complements of subspaces, II, Proceedings of the American Mathematical Society,* 125 (1997), 251–254.

[32] W. E. Clark and B. Shekhtman, *Covering by complements of subspaces, Linear and Multilinear Algebra,* 40 (1997), 1–13.

[33] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Boca Raton, Florida: Chapman and Hall/CRC, 2007.

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

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

[36] P. Delsarte, *An algebraic approach to the association schemes of coding theory, Philips Res. Repts. Suppl.,* 10 (1973), 1–97.

[37] P. Delsarte, *Association schemes and t-designs in regular semilattices, Journal of Combinatorial Theory, Series A,* 20 (1976), 230–243.

[38] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory, Journal of Combinatorial Theory, Series A,* 25 (1978), 226–241.

[39] D. A. Drake and J. W. Freeman, *Partial t-spreads and group constructible (s, r, μ)-nets, Journal of Geometry,* 13 (1979), 210–216.

[40] J. Eisfeld and K. Metsch, *Blocking s-dimensional subspaces by lines in $PG(2s, q)$, Combinatorica,* 17 (1997), 151–162.

[41] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence *The maximum size of a maximal 3-spread in a finite vector space over GF(2) Designs, Codes, and Cryptography,* 54 (2010) 101–107.

[42] T. Etzion, *New Lower Bounds for Asymmetric and Unidirectional Codes, IEEE Trans. Inform. Theory*, 37 (1991), 1696–1704.

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

[44] T. Etzion *Covering of subspaces by subspaces, arxiv.org/abs/1111.4319*, November 2011. *Designs, Codes, and Cryptography,* to appear.

[45] T. Etzion *Partial k-Parallelisms in Finite Projective Spaces, arxiv.org/abs/1302.3629*, February 2013.

[46] T. Etzion *The q-Analog of the Middle Levels Problem, arxiv.org/abs/1303.7110*, March 2013.

[47] T. Etzion and P. R. J. Östergård, *Greedy and Heuristic Algorithms for Codes and Colorings, IEEE Trans. Inform. Theory*, 44 (1998), 382–388. (see correction in 44 (1992), 1183–1184).

[48] T. Etzion and N. Silberstein, *Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams, IEEE Trans. Inform. Theory*, 55 (2009), 2909–2919.

[49] T. Etzion and N. Silberstein, *Codes and Designs Related to Lifted MRD Codes, IEEE Trans. Inform. Theory*, 59 (2013), 1004–1017.

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

[51] T. Etzion and A. Vardy, *Automorphisms of codes in the Grassmann scheme, arxiv.org/abs/1210.5724*, October 2012.

[52] T. Etzion and A. Vardy, *On q-Analogs for Steiner Systems and Covering Designs, Advances in Mathematics of Communications*, 5 (2011), 161–176.

[53] P. Frankl and R. M. Wilson, *The Erdős-Ko-Rado theorem for vector spaces,, Journal of Combinatorial Theory, Series A,* 43 (1986), 228–236.

[54] E. M. Gabidulin, *Theory of codes with maximum rank distance, Problems of Information Transmission*, 21 (1985), 1–12.

[55] M. Gadouleau and Z. Yan, *Packing and covering properties of subspace codes for error control in random linear network coding, IEEE Trans. Inform. Theory*, 56 (2010), 2097–2108.

[56] M. Gadouleau and Z. Yan, *Constant-rank codes and their connection to constant-dimension codes, IEEE Trans. Inform. Theory*, 56 (2010), 3207–3216.

[57] A. Ghatak, *Subspace codes for random networks based on Plücker coordinates and Schubert cells*, *arxiv.org/abs/1301.6362*, January 2013.

[58] E. Gorla, F. Manganiello, and J. Rosenthal, *An Algebraic Approach for Decoding Spread Codes*, *Advances in Mathematics of Communications*, 6 (2012), 443–466.

[59] V. Guruswami, S. Narayanan, and C. Wang, *List decoding subspace codes from insertions and deletions*, *arxiv.org/abs/1202.0535*, February 2012.

[60] V. Guruswami and C. Xing, *List-decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound*, *Electronic Colloquium on Computational Complexity*, 19 (2012), 1–37.

[61] J. I. Hall, *Bounds for equididtant codes and partial projective planes*, *Discrete Mathematics*, 17 (1977), 85–94.

[62] J. P. Hansen *Equidistant linear codes with maximal error-protection from Veronese varieties*, *arxiv.org/abs/1207.2083*, July 2012.

[63] J. P. Hansen *Osculating spaces of varieties and linear network codes*, *arxiv.org/abs/1210.7961*, October 2012.

[64] J. P. Hansen *Forms and linear network codes*, *arxiv.org/abs/1303.1626*, March 2013.

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

[66] W. N. Hsieh, *Intersection theorems for systems of finite vector spaces*, *Discrete Math.*, 12 (1975), 1–16.

[67] T. Itoh, *A new family of 2-designs over GF(q) admitting* $SL_m(q^\ell)$, *Geometriae Dedicata,* 69 (1998), 261–286.

[68] A. Khaleghi and F. R. Kschischang, *Projective space codes for injection metric*, *arxiv.org/abs/0904.0813*, February 2009.

[69] A. Khaleghi, D. Silva, and F. R. Kschischang, *Subspace codes,* in Coding and Cryptography, *Lecture Notes in Computer Science,* 5921 (2009), 1–21.

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

[71] A. Kohnert and S. Kurz, *Construction of large constant dimension codes with a prescribed minimum distance*, *Lecture Notes Computer Science*, 5393 (2008), 31–42.

[72] G. Lunardon, *Normal spreads, Geometriae Dedicata,* 75 (1999), 245–261.

[73] H. Mahdavifar and A. Vardy, *Algebraic list-decoding on the operator channel,* in proc. of *ISIT 2010*, pp. 1193–1197.

[74] H. Mahdavifar and A. Vardy, *Algebraic list-decoding of subspace codes with multiplicities,* in proc. of *49th Annual Allerton Conference*, (2011), 1430–1437.

[75] H. Mahdavifar and A. Vardy, *Algebraic list-decoding of subspace codes, arxiv.org/abs/1202.0338*, Ffebruary 2012.

[76] H. Mahdavifar and A. Vardy, *List-decoding of subspace codes and rank-metric codes up to Singleton bound,* in proc. of *ISIT 2012*, pp. 1188–1192.

[77] F. Manganiello, E. Gorla, and J. Rosenthal, *Spread codes and spread decoding in network coding,* in proc. of *ISIT 2008*, pp. 881–885.

[78] F. Manganiello, A.-L. Trautmann, and J. Rosenthal, *On conjugacy classes of subgroups of the general linear group and cyclic orbit codes*, in proc. of *ISIT 2011*, pp. 1916–1920.

[79] W. J. Martin and X. J. Zhu, *Anticodes for the Grassmann and bilinear forms graphs, Designs, Codes, and Cryptography,* 6 (1995), 73–79.

[80] Y. Medvedeva, *Fast enumeration for Grassmannian space,* in proc. of *Problems of Redundancy in Information and Control Systems 2012*, pp. 48–52.

[81] K. Metsch, *Bose-Burton type theorems for finite projective, affine and polar spaces,* in J.D. Lamb and D.A. Preece, Eds., *Surveys in Combinatorics, 1999*, London Math. Soc. Lecture Note Ser. 267, Cambridge Univ. Press, Cambridge, pp. 137–166, 1999.

[82] K. Metsch, *Blocking sets in projective spaces and polar spaces, Journal of Geometry,* 76 (2003), 216–232.

[83] K. Metsch, *Blocking subspaces by lines in PG(n, q), Combinatorica,* 24 (2004), 459–486.

[84] M. Miyakawa, A. Munemasa, and S. Yoshiara, *On a class of small 2-designs over GF(q), Journal Combinatorial Designs,* 3 (1995), 61–77.

[85] J. Rosenthal and A.-L. Trautmann, *Decoding of subspace codes, a problem of Schubert calculus over finite fields, arxiv.org/abs/1209.2887*, September 2012.

[86] R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inform. Theory*, 37 (1991), 328–336.

[87] J. Sarmiento, *On point-cyclic resolutions of the* $2-(63,7,15)$ *design associated with PG(5,2), Graphs and Comb.*, 18 (2002), 621–632.

[88] C. Savage, *A survey of combinatorial Gray codes, SIAM Review,* 39 (1997), 605–629.

[89] C. D. Savage and P. Winkler, *Monotone Gray codes and the Middle levels problem, Journal of Combinatorial Theory, Series A*, 70 (1995), 230–248.

[90] N. Schrijver, *A comparison of the Delsarte and Lovász bound, IEEE Trans. Inform. Theory*, 25 (1979), 425–429.

[91] N. Schrijver, *New code upper bounds from the Terwilliger algebra and semide nite programming*, *IEEE Trans. Inform. Theory*, 5 (2005), 2859–2866.

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

[93] M. Schwartz and T. Etzion, *Codes and anticodes in the Grassman graph, Journal Combinatorial Theory, Series A,* 97 (2002), 27–42.

[94] V. P. Shilo, *New lower bounds of the size of error-correcting codes for the Z-channel*, *Cybernetics and Systems Analysis*, 38 (2002), 13–16.

[95] N. Silberstein and T. Etzion, *Enumerative coding for Grassmannian space*, *IEEE Trans. Inform. Theory*, 57 (2011), 365–374.

[96] N. Silberstein and T. Etzion, *Large constant dimension codes and lexicodes*, *Advances of Mathematics in Communications*, 5 (2011), 177–189.

[97] N. Silberstein and A.-L. Trautmann, *New lower bounds for constant dimension codes*, *arxiv.org/abs/1301.5961*, January 2013.

[98] D. Silva, F. R. Kschischang, and R. Koetter, *A rank-metric approach to error control in random network coding, IEEE Trans. Inform. Theory*, 54 (2008), 3951–3967.

[99] D. Silva and F. R. Kschischang, *On metrics for error-correction in network coding, IEEE Trans. Inform. Theory*, 55 (2009), 5479–5490.

[100] V. Skachek, *Recursive code construction for random networks, IEEE Trans. Inform. Theory*, 56 (2010), 1378–1382.

[101] V. Skachek, O. Milenkovic, and A. Nedić, *Hybrid noncoherent network coding, IEEE Trans. Inform. Theory*, 59 (2013), 3317–3331.

[102] R. P. Stanley, *Enumerative Combinatorics, volume 1*, Wadsworth, 1986.

[103] N. Sendrier, *On the dimension of the hull, SIAM J. Discr. Math.,* 10 91997), 282–293.

[104] H. Suzuki, *2-designs over GF(2^m), Graphs and Combinatorics,* 6 (1990), 293–296.

[105] H. Suzuki, *2-designs over GF(q), Graphs and Combinatorics,* 8 (1992), 381–389.

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

[107] S. Thomas, *Designs and partial geometries over finite fields, Geometriae Dedicata,* 63 (1996), 247–253.

[108] A.-L. Trautmann, *isometry and automorphisms of constant dimension codes*, *Advances of Mathematics in Communications*, 7 (2013), 147–160.

[109] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, *Cyclic Orbit Codes, arxiv.org/abs/1112.1238*, December 2011.

[110] A.-L. Trautmann, F. Manganiello, and J. Rosenthal, *Orbit codes - a new concept in the area of network coding*, *Information Theory Workshop*, pp. 1-4, Dublin, Ireland, August 2010.

[111] A.-L. Trautmann, N. Silberstein, and J. Rosenthal, *List decoding of lifted Gabidulin codes via the Plücker embedding*, *arxiv.org/abs/1301.2165*, January 2013.

[112] A.-L. Trautmann and J. Rosenthal, *New improvements on the echelon-Ferrers construction,* in Proc. of *Int. Symp. on Math. Theory of Networks and Systems*, pp. 405-408, July 2010.

[113] A.-L. Trautmann and J. Rosenthal, *Decoding of subspace codes, a problem of schubert calculus over finite fields*, *arxiv.org/abs/1209.2887*, September 2012.

[114] A.-L. Trautmann and J. Rosenthal, *A complete characterization of irreducible cyclic orbit codes and their Plücker embedding*, *Designs, Codes, and Cryptography,* 66 (2013), 275–289.

[115] J. H. van Lint and R. M. Wilson, *A course in Combinatorics*, Cambridge University Press, 1992.

[116] H. Wang, C. Xing, and R. M. Safavi-Naini, *Linear authentication codes: bounds and constructions*, *IEEE Trans. Inform. Theory*, 49 (2003), 866–872.

[117] S.-T. Xia and F.-W. Fu, *ohnson type bounds on constant dimension codes*, *Designs, Codes, and Cryptography,* 50 (2009), 163–172.

[118] E. Yaakobi, M. Schwartz, M. Langberg, and J. Bruck, *Sequence reconstruction for Grasmann graphs and Permutations*, to be presented in *ISIT 2013*.

[119] G. V. Zaicev, V. A. Zinoviev, and N. V. Semakov, *Interrelations of Preparata and Hamming codes and extension of Hamming codes to new double error-correcting codes,* in *Proc. 2nd inter. symp. information theory,* Budapest (1971), 257–263.