Ghent University
Faculty of Sciences
Department of Mathematics

Random network coding and designs over $\mathbb{F}_q$

Lien Lambert

Academic year 2012-2013

Supervisor: Prof. Dr. L. Storme

Master dissertation submitted to the Faculty of Sciences to obtain the degree of Master of Science in Mathematics: Pure Mathematics

Preface

About a year ago, I asked Prof. Dr. Leo Storme for a possible subject for my master dissertation, preferably in my favourite mathematical domains, i.e. coding theory and geometry. He suggested me among others to consider random network coding, a recently established powerful concept for information transmission in a network, with widespread applications for communication networks like the Internet, wireless communication systems and cloud computing. In the recent award-winning article of Kötter and Kschischang ([28]), the network is viewed as a mechanism of transmitting not packets or vectors but rather the subspace that these packets span, which leads to a new kind of coding theory employing subspace codes. After reading this article I was very enthusiastic to look into this subject in more depth, to explore the links between new and traditional concepts in different domains and to try to describe this in my thesis, which can be seen as an introduction to the mathematical part of random network coding and designs over $\mathbb{F}_q$.

Furthermore, I like to mention COST Action IC1104 (see [9] or [10]), which sets up a European research network about random network coding and designs over $\mathbb{F}_q$ and its aim is to bring together experts from pure and applied mathematics, computer science, and electrical engineering, who are working in the areas of discrete mathematics, coding theory, information theory, and related fields.

The importance of collaboration is also clear from the quote of the American psychologist Howard Gardiner, representing the vision of the COST Action ([11]):

> "The tools from any one discipline are often insufficient for understanding and solving real world problems highlighting the need for interdisciplinary expertise and problem-centered teams of people working on common goals."

Hereby, I had the opportunity to participate in the First European Training School on Network Coding within the COST Action, which took place on February 4-8, 2013, at the Autonomous University of Barcelona. Thanks to the interesting talks and useful practical sessions with researchers, such as Kschischang and Etzion, I acquired a better and broader view on the possibilities of this subject, gained new insight in the matter and found the motivation and inspiration to proceed with my work.

I have written down the results of my discoveries in the wonderful world of network codes and q-designs in this master dissertation, of which I will now shortly elucidate the different chapters.

The aim of the first chapter is to introduce the basic concepts needed in the subsequent chapters and to make it possible to establish a link between the concepts, theorems and

proofs of traditional coding theory, design theory and graph theory. As a matter of fact, a lot of new concepts are the q-analogues or q-generalizations of classical theorems, identities or expressions.

The second chapter handles the general idea of random network coding and shows that codes in $\mathcal{P}_q(n)$ are precisely what is needed for error-correction in networks: an (n, M, d)-code can correct any t packet errors and any ρ erasures emerged anywhere in the network as long as $2(t + \rho) < d$. This motivates our interest in such codes and in a sense, one would like to rederive as much as possible of the classical coding theory in the context of $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n, k)$ with the subspace metric.

In Chapter 3, we consider the main coding theory problem for codes in projective space. In this chapter we focus in particular on the special case of constant-dimension codes. We want to find the largest number of codewords for given parameters and therefore, we discuss bounds on these values, such as the sphere-packing bound or Singleton bound. Furthermore, the (non)existence of perfect codes will also be handled.

Strongly related with codes are designs. In the fourth chapter, we define covering designs $\mathscr{C}_q(n, k, t)$, Steiner structures $\mathscr{S}_q(t, k, n)$ and Turán designs $\mathscr{T}_q(n, k, t)$ of which the existence and bounds on their sizes are discussed. Since Steiner structures are optimal covering designs, most of our attention is devoted to these. Hereby, we will also discuss the recent and important result from [5] about the existence of Steiner structures $\mathscr{S}_2(2, 3, 13)$ and related Steiner systems $\mathcal{S}(3, 8, 8192)$.

In the last chapter, (partial) spreads and (partial) spread codes are discussed in the context of coding theory, design theory and projective geometry. For instance, a construction of Beutelspacher of partial spreads in projective geometry leads to a useful partial spread code $\mathcal{C}_q(k, n; p, p')$, of which we discuss the construction and some properties, and a decoding algorithm for partial spread codes. We also consider another example of a partial spread. Although it is still difficult to see if there would be applications of this partial spread from the decoding point of view, we could give a geometrical description of the corresponding set of holes, found by a computer search made by Peter Vandendriessche.

But there are still bounds to improve, more q-analogues to be made and possibly even other constructions of partial spreads or new Steiner structures to be found... I hope that maybe the reader of this work will be given a taste for this fascinating subject and be encouraged to read more about it and to do research on this topic.

By making this english dissertation available for the COST Action, I hope I can hereby make a contribution to the further development of random network coding and designs over $\mathbb{F}_q$.

Permission for usage

Lien Lambert Aalter, May 26, 2013

Acknowledgements

Many people have supported me during my studies and in particularly during the writing of this thesis. I would very much like to thank everyone who has contributed in any way to the realisation of this work.

First of all, this thesis would not have been possible without the help, enthusiasm and guidance of my supervisor Prof. Dr. Leo Storme. I am very thankful that he offered me such an interesting subject, that he was always willing to give an enlightening explanation and that he carefully read and corrected my results.

Not only did he help me to gain mathematical insights throughout our discussions, he also emphasised the importance of collaboration and being open-minded. On this subject I am very grateful that he gave me the opportunity to attend the Training School in Barcelona. There, I could experience that mathematics are very much alive and that by expanding our horizons and by broadening our views to other domains of mathematics, we can realise great results. Therefore, I would also like to thank the organisation of COST Action IC1104, in particular for their financial support, and all the attendees of the Training School in Barcelona for the inspiration, suggestions and help they gave me.

But in fact, throughout my entire career at the University of Ghent, professors, assistants and fellow students taught me, apart from the amounts of interesting knowledge and mathematical luggage, a spirit of cooperation, which I will live by throughout my further career. I am grateful that I could study in such a warm and dynamical atmosphere that creates opportunities to communicate with people to reach a higher level.

In particular for my thesis, I would like to have a special word of thank to Maarten De Boeck, Dieter De Smedt, Roel Verbelen, Nigel Vinckier and other friends who helped me with mathematical, LaTeX, linguistic or other problems and supported me throughout this year.

Last but not least, I want to express my gratitude to my parents, family and friends, who gave me the opportunity to follow my dreams and made me the person I am today, the person, who is proud to present to you, dear reader, this thesis about random network coding and designs over $\mathbb{F}_q$.

Lien Lambert Aalter, May 26, 2013

Contents

Chapter 1

Preliminaries

In this first chapter, we want to introduce some definitions, properties, examples ... and define all basic concepts needed in the chapters that follow. Since in this thesis we want to make a link between classical coding theory and random network coding, we start in the first section with some important basic information, based on [22] and [30]. Since there is a close relation with coding theory, we also consider designs, for which we used [39]. Furthermore, there is a small section about graph theory, in order to define two important distance-regular graphs, i.e. the Hamming graph and the Johnson graph. Therefore, we made use of [40] for the basic concepts and [6] for the more advanced information. To conclude this chapter, we introduce the notion of a q-analogue and relate this to the Erdős-Ko-Rado problems. This section, based on [12] and [40], points the way to the subsequent chapters, since we will see that a lot of concepts for random network coding are in fact q-analogues of concepts in classical coding theory, design theory, etc.

1.1 Coding theory

1.1.1 Error-correcting codes and the Hamming distance

When messages are transmitted through a noisy communication channel, e.g. a telephone line or a satellite communication link, some errors may occur. The data received can be different from what is sent, due to for example human error, imperfections in equipment etc. If there has been a mistake in the transmission, some codes can detect this. Or even better, some codes can correct these errors, the so called error-correcting codes. The task of an error-correcting code is to encode the data, by adding a certain amount of redundancy to the message, so that the original message can be recovered if (not too many) errors have occurred.

Definition 1.1.1. A ***q-ary code*** $\mathcal{C}$ is a given set of sequences of symbols from a set $F_q = \{\lambda_1, \ldots, \lambda_q\}$ of q distinct elements. The set F_q is called the alphabet and usually, we choose $F_q = \{0, \ldots, q-1\}$. If q is a prime power, we take the finite field $\mathbb{F}_q$ as alphabet. The elements of $\mathcal{C}$ are called the ***codewords***.

Definition 1.1.2. If a q-ary code $\mathcal{C}$ is a subset of $(F_q)^n$, i.e. a code $\mathcal{C}$ of which each codeword has the same number n of symbols, we say that $\mathcal{C}$ is a ***block code of length n over F_q***.

In this introduction, we shall restrict our attention to block codes. So by 'code' we shall always mean 'block code'.

Since for error-correcting codes it is important to know 'how far' a received vector is from a transmitted vector or which codeword is 'the closest' to a received vector, we need a notion of 'distance'. We make this concept precise by the distance function $d : (F_q)^n \times (F_q)^n \to \mathbb{Z}_+$, with $\mathbb{Z}_+$ the set of nonnegative integers.

Definition 1.1.3. The ***Hamming distance*** between two vectors x and y of $(F_q)^n$, denoted by $\boldsymbol{d(x, y)}$, is the number of places in which they differ.

The Hamming distance is a metric because for all $x, y, z \in (F_q)^n$ it satisfies the three conditions (see e.g. [22]):

(i) $d(x, y) \geqslant 0$ and equality holds if and only if $x = y$,

(ii) $d(x, y) = d(y, x)$,

(iii) $d(x, y) \leqslant d(x, z) + d(z, y)$.

Definition 1.1.4. The space of all q-ary vectors of a given length n and of which the distance between these vectors is measured by the Hamming distance, is called the ***Hamming space $\mathcal{H}(n, q)$***. The size of this space is q^n.

Definition 1.1.5. The ***minimum distance*** of a code $\mathcal{C}$, denoted by $\boldsymbol{d(\mathcal{C})}$, is the smallest of the distances between distinct codewords, i.e.

$$d(\mathcal{C}) = \min\{d(x, y) | x, y \in \mathcal{C}, x \neq y\}.$$

Definition 1.1.6. An ***(n, M, d)-code*** is a code of length n, containing M codewords and having minimum distance $d(\mathcal{C}) = d$. The set af all q-ary codes with length n and minimum distance d is denoted as $\boldsymbol{\mathcal{C}_q(n, d)}$.

The minimum distance of a code $\mathcal{C}$ gives a measure of how good this code is at error detection or error correction. The following theorem shows the importance of this concept.

Theorem 1.1.7. *Let C be an (n, M, d)-code.*

(i) If $d = s + 1$, then $\mathcal{C}$ can detect up to s errors in a codeword and we call $\mathcal{C}$ an ***s*-detecting code**.

(ii) If $d = 2t + 1$ or $d = 2t + 2$, then $\mathcal{C}$ can correct up to t errors in a codeword and we call $\mathcal{C}$ a ***t*-correcting code**.

Definition 1.1.8. A ***minimum-distance decoder*** for a code $\mathcal{C}$ is one that takes the output vector x and returns a nearest codeword $y \in \mathcal{C}$, i.e. a codeword $y \in \mathcal{C}$ satisfying, $\forall y' \in \mathcal{C}, d(x, y) \leqslant d(x, y')$.

It follows from Theorem 1.1.7, that if for a code $\mathcal{C}$ with $d(\mathcal{C}) = d$ and the number of errors is

$$t \leqslant \left\lfloor \frac{d-1}{2} \right\rfloor,$$

then the minimum-distance decoder will always return the original transmitted codeword.

A good (n, M, d)-code is a code with small n, for fast transmission of codewords, large M, for a transmission of a wide variety of messages, and large d, to correct many errors. Maximizing M and d are conflicting aims and a compromise has to be found. The so called ***main coding theory problem*** is to optimize one of the parameter n, M, d for given values of the other two. Usually, the problem is to find the largest code of given n and d.

Definition 1.1.9. The largest value of M such that there exists a q-ary (n, M, d)-code is denoted by $\boldsymbol{A_q(n, d)}$, so

$$A_q(n, d) = \max_{\mathcal{C} \in \mathcal{C}_q(n,d)} |\mathcal{C}|.$$

A way of handling the main coding theory problem is to find bounds for $A_q(n, d)$ for specific values of n, d, q. This is a very important research area in coding theory, see for instance Appendix A of [30] for tables of the best codes known.

Next to the length, we define another parameter for a codeword.

Definition 1.1.10. Let $x \in (F_q)^n$, with $F_q = \{0, \lambda_1, \ldots, \lambda_{q-1}\}$, the ***weight*** of x, denoted by $\boldsymbol{w(x)}$, is the number of nonzero entries of the vector x. The ***minimum weight*** $\boldsymbol{w(\mathcal{C})}$ of a code is the smallest of the weights of the nonzero codewords of $\mathcal{C}$.

From now on, we assume that the alphabet F_q is the finite field $\mathbb{F}_q$, where q is a prime power, and we see $\mathbb{F}_q^n$ as the vector space $V(n, q)$.

There is a nice link between the Hamming distance of two codewords $x, y \in \mathbb{F}_q^n$ and the weight of their difference, since the vector $x - y$ has nonzero entries in precisely those places where x and y differ.

Theorem 1.1.11. *Let $x, y \in \mathbb{F}_q^n$, then $d(x, y) = w(x - y)$.*

Definition 1.1.12. The subspace of the Hamming space of all binary vectors of a given length n with a fixed weight w is called the ***Johnson space*** and denoted by $\boldsymbol{\mathcal{J}(n, w)}$. The size of this space is $\binom{n}{w}$.

Now, consider an important subset of $\mathcal{C}_q(n, d)$.

Definition 1.1.13. A q-ary (n, M, d)-code $\mathcal{C}$ such that every element has exactly w nonzero entries, is a ***constant-weight code*** with weight w and we say that $\mathcal{C}$ is an $\boldsymbol{(n, M, d, w)}$***-code***. Such a code is an element of the set $\boldsymbol{\mathcal{C}_q(n, d, w)}$, the set of all codes in $\mathcal{C}_q(n, d)$ such that the weight of every codeword is w.

Definition 1.1.14. The largest value of M such that there exists a constant-weight (n, M, d)-code $\mathcal{C}$ with weight w is denoted by $\boldsymbol{A_q(n, d, w)}$, so

$$A_q(n, d, w) = \max_{\mathcal{C} \in \mathcal{C}_q(n,d,w)} |\mathcal{C}|.$$

Most of the time constant-weight codes will be studied for $q = 2$, i.e. codes for which every element is a vector of the Johnson space $\mathcal{J}(n, w)$, for some weight w, and sometimes in literature, they refer to constant-weight codes if they mean the binary constant-weight codes.

Also for constant-weight codes, a lot of researchers are investigating $A_q(n, d, w)$ for specific parameters (see e.g. [30]).

We will finish this first subsection with another relation between the Hamming distance and the weight in the binary case. Therefore, we need the notion of the intersection of two vectors.

Definition 1.1.15. Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two vectors of length n over $\mathbb{F}_2 = \{0, 1\}$. Then the ***intersection*** $\boldsymbol{x \cap y}$ is the vector in $\mathbb{F}_2^n$ defined by

$$x \cap y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

Theorem 1.1.16. *Let $x, y \in \mathbb{F}_2^n$, then*

$$d(x, y) = w(x) + w(y) - 2w(x \cap y).$$

For the case of binary codes, this theorem gives in fact a new definition of the Hamming distance. The structure of this characterisation is very similar to that of the definition of the Levenshtein distance (1.1.1) and the subspace distance (2.2.2) and shows a certain connection between these metrics.

1.1.2 Linear codes and the Hamming codes

Definition 1.1.17. A ***linear code*** over $\mathbb{F}_q$ is a subspace of $V(n, q)$. Thus a subset $\mathcal{C}$ of $V(n, q)$ is a linear code if and only if

(i) $u + v \in \mathcal{C}$, for all $u, v \in \mathcal{C}$,

(ii) $a \cdot u \in \mathcal{C}$, for all $u \in \mathcal{C}$ and $a \in \mathbb{F}_q$.

If $\mathcal{C}$ is a k-dimensional subspace of $V(n, q)$, then the linear code $\mathcal{C}$ is called an ***$[n, k]$-code***. If we want to specify the minimum distance d of $\mathcal{C}$, we write $[n, k, d]$-code.

One of the most useful properties of a linear code is that its minimum distance is equal to the minimum of the weights of the nonzero codewords, stated in the following theorem.

Theorem 1.1.18. *Let $\mathcal{C}$ be a linear code, then $d(\mathcal{C}) = w(\mathcal{C})$.*

Definition 1.1.19. A $(k \times n)$-matrix whose rows form a basis of a linear $[n, k]$-code is called a ***generator matrix*** of the code. Note that a linear code is defined by its generator matrix.

Definition 1.1.20. The ***standard form*** of a generator matrix G of the $[n, k]$-code $\mathcal{C}$ is of the form

$$\begin{bmatrix} I_k & A \end{bmatrix},$$

with I_k the identity matrix of order k and A a $(k \times (n - k))$-matrix.

One way to specify a linear code is by its generator matrix. Another important way of defining a linear code is by a parity-check matrix. First we need some other concepts.

Note that the inner product $u \cdot v$ of the vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ is the scalar $u_1v_1 + u_2v_2 + \ldots + u_nv_n$, and if $u \cdot v = 0$, u and v are called ***orthogonal***.

Definition 1.1.21. Given a linear $[n, k]$-code $\mathcal{C}$, the ***dual code of*** $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined to be the set of those vectors of $V(n, q)$ which are orthogonal to every codeword of $\mathcal{C}$, i.e.

$$\mathcal{C}^\perp := \{v \in V(n, q) |\, v \cdot u = 0, \text{ for all } u \in \mathcal{C}\}.$$

Theorem 1.1.22. *Suppose that $\mathcal{C}$ is an $[n, k]$-code of $\mathbb{F}_q$, then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is a linear $[n, n - k]$-code.*

Definition 1.1.23. A ***parity-check matrix*** H for an $[n, k]$-code $\mathcal{C}$ is a generator matrix of $\mathcal{C}^\perp$.

It follows that H is an $((n - k) \times n)$-matrix satisfying $GH^T = 0$, with 0 an all-zero matrix, and that

$$\mathcal{C} = \{x \in V(n, q) |\, xH^T = 0\}.$$

In this way, any linear code is completely specified by a parity-check matrix.

Definition 1.1.24. A parity-check matrix H is said to be in ***standard form*** if

$$H = \begin{bmatrix} B & I_k \end{bmatrix}.$$

The next fundamental theorem establishes the relationship between the minimum distance of a linear code and a linear independence property of the columns of a parity-check matrix.

Theorem 1.1.25. *Suppose that $\mathcal{C}$ is a linear $[n, k]$-code over $\mathbb{F}_q$ with parity-check matrix H. Then the minimum distance of $\mathcal{C}$ is d if and only if any $d - 1$ columns of H are linearly independent and there exist d linearly dependent columns.*

An important family of linear codes which are single-error-correcting codes and easy to encode and decode, are the ***Hamming codes***. A Hamming code is most conveniently defined by specifying its parity-check matrix.

Definition 1.1.26. Let r be a positive integer and let H be an $(r \times (2^r - 1))$-matrix whose columns are the distinct nonzero vectors of $V(r, 2)$. Then the code having H as its parity-check matrix is called a ***binary Hamming code*** and is denoted by $\mathbf{Ham}\,(r, 2)$.

Theorem 1.1.27. *The binary Hamming code* $\mathrm{Ham}(r, 2)$*, $r \geqslant 2$, is a $[2^r - 1, 2^r - 1 - r, 3]$-code (and hence a single-error-correcting code).*

The Hamming code $\mathrm{Ham}(r, 2)$ has length $n = 2^r - 1$ and dimension $k = n - r$. This number r is the number of check symbols in each codeword and is also known as the ***redundancy*** of the code.

Definition 1.1.28. The ***extended binary Hamming code*** $\widehat{\mathbf{Ham}}\,\mathbf{(r,2)}$ is the code obtained from $\mathrm{Ham}(r,2)$ by adding an overall parity-check, i.e. if H is the parity-check matrix for $\mathrm{Ham}(r,2)$, the parity-check matrix $\widehat{H}$ for the extended code is

$$\begin{bmatrix} & & 0 \\ & H & \vdots \\ & & 0 \\ 1 & \cdots & 1 \end{bmatrix}.$$

Theorem 1.1.29. *The extended binary Hamming code* $\widehat{\mathrm{Ham}}(r,2)$, $r \geqslant 2$, *is a linear* $[2^r, 2^r-1-r, 4]$*-code.*

Now we want to extend the definition of a binary Hamming code to the definition of a Hamming code over a finite field $\mathbb{F}_q$. In order that $\mathcal{C}$ be a linear code with minimum distance 3, by Theorem 1.1.25, we require that any two columns of a parity-check matrix H are linearly independent. Therefore, the columns must be nonzero and no column can be a scalar multiple of another column. To construct an $[n, n-r, 3]$-code over $\mathbb{F}_q$, for a fixed redundancy r and with n as large as possible, we need a set of nonzero vectors of $V(r,q)$ such that none is a scalar multiple of another. This is the same as taking all different points of the $(r-1)$-dimensional projective space $\mathrm{PG}(r-1,q)$. From this observation, we get the following definition.

Definition 1.1.30. Let r be a positive integer and let H be an $(r \times n)$-matrix, with $n = \frac{q^r-1}{q-1}$, whose columns are the n different points of the $(r-1)$-dimensional projective space $\mathrm{PG}(r-1,q)$. Then the code having H as its parity-check matrix is called a ***q-ary Hamming code*** and is denoted by $\mathbf{Ham}\,\mathbf{(r,q)}$.

1.1.3 Bounds on codes in the Hamming space

In search of the values $A_q(n,d)$ and $A_q(n,d,w)$ for specific values for q, n, d, w, bounds arise to restrict the intervals to which these values belong. In this subsection, we give some important bounds, of which we will try to give an analogon for the case of random network codes in Chapter 3.

1.1.3.1 Sphere-packing bound and sphere-covering bound

Theorem 1.1.7 can also be interpreted in a more visual way. Therefore, we introduce the next definition of a sphere.

Definition 1.1.31. For any vector $x \in \mathbb{F}_q^n$ and any integer $r \geqslant 0$, the ***sphere*** of radius r and center x is the set

$$S(x,r) \coloneqq \{y \in \mathbb{F}_q^n | d(x,y) \leqslant r\}.$$

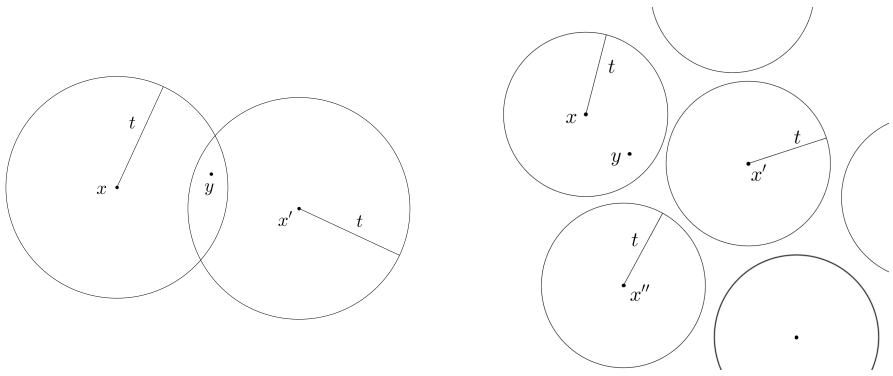
Lemma 1.1.32. *The number of vectors in a sphere* $S(x,r)$ *of center* $x \in \mathbb{F}_q^n$ *and radius* r, $0 \leqslant r \leqslant n$, *is independent of* x *and equals*

$$|S(x,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

If $\mathcal{C}$ is a code with $d(\mathcal{C}) \geqslant 2t+1$, then the spheres of radius t centered on the codewords of $\mathcal{C}$ are pairwise disjoint, since if a vector y were in both $S(x,t)$ and $S(x',t)$, for $x, x' \in \mathcal{C}$, $x \neq x'$ (see Figure 1.1a), then by the triangle inequality we would have

$$d(x,x') \leqslant d(x,y) + d(x',y) \leqslant t + t = 2t,$$

a contradiction to $d(\mathcal{C}) \geqslant 2t+1$. So if we send a codeword x and we make at most t errors, then the received vector y belongs to the sphere $S(x,t)$ and the minimum-distance decoder returns x. This is shown in Figure 1.1b.



(a) **(b)**

Figure 1.1: Visualisation of Theorem 1.1.7

This way of viewing gives us an upper bound on the numbers of codewords for an (n, M, d)-code and is therefore called the sphere-packing bound.

Theorem 1.1.33 (Sphere-packing bound or Hamming bound)**.** *A q-ary (n, M, d)-code with $d = 2t+1$ or $d = 2t+2$ satisfies*

$$M \left[\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right] \leqslant q^n$$

or, in other words,

$$A_q(n,d) \leqslant \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Definition 1.1.34. A code which achieves the sphere-packing bound is called a ***perfect code***.

The binary repetition codes of length n, n odd, are perfect $(n, 2, n)$-codes in the Hamming space. In the binary Johnson space $\mathcal{J}(2n, n)$, n odd, two codewords x, y with for x a one on n fixed positions and for y a zero on these n positions, form a perfect code. Such codes, together with the codes which contain only one codeword or which contain all vectors of $\mathbb{F}_q^n$, are called the ***trivial perfect codes***. The problem of finding all perfect codes has been a big challenge, and is still a challenge, in coding theory.

Examples of perfect codes are all q-ary Hamming codes.

The sphere-packing bound gives an upper bound on $A_q(n,d)$. With the next theorem, again by using spheres to prove it, we give a lower bound on the maximum number M for an (n,M,d)-code.

Theorem 1.1.35 (Sphere-covering bound)**.** *For an integer $q \geqslant 2$ and integers n, d such that $1 \leqslant d \leqslant n$, we have*

$$A_q(n,d) \geqslant \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

Remark 1.1.36. In the literature, the previous bound is also well known as (the weaker version of) the ***Gilbert-Varshamov bound***.

1.1.3.2 Singleton bound

Another bound on the maximum number of codewords for an (n,M,d)-code is the bound of Singleton. The technique to prove this theorem is by ***puncturing*** the code $d-1$ times, i.e. by deleting the last $d-1$ coordinates, and observing that the original code has as much codewords as the obtained punctured code and hence, cannot have more codewords than vectors in $\mathbb{F}_q^{n-d+1}$.

Theorem 1.1.37 (Singleton bound)**.** *For any integers $q \geqslant 2$, $1 \leqslant d \leqslant n$, we have*

$$A_q(n,d) \leqslant q^{n-d+1}.$$

1.1.3.3 Johnson bounds

For the Johnson bounds, we restrict to the case of binary codes with weight w. This means that we give bounds for $A_2(n,d,w)$, based on Chapter 17 of [30].

Theorem 1.1.38.

$$A_2(n,d,w) \leqslant \left\lfloor \frac{n}{w} A_2(n-1,d,w-1) \right\rfloor$$

Proof. Let $\mathcal{C}$ be a code with $|\mathcal{C}| = A_2(n,d,w)$. Consider the codewords of $\mathcal{C}$ which have a 1 in the ith position. If this coordinate is deleted, we obtain a new code with length $n-1$, distance larger than or equal to d and constant weight $w-1$. Therefore the number of such codewords is less than or equal to $A_2(n-1,d,w-1)$. Since we can do this observation for every position, the total number of 1's in the original code satisfies

$$w|\mathcal{C}| = wA_2(n,d,w) \leqslant nA_2(n-1,d,w-1).$$

Since $A_2(n,d,w)$ is an integer, the theorem follows. □

Iterating this theorem gives us the following corollary.

Corollary 1.1.39.

$$A_2(n,2\delta,w) \leqslant \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \cdots \left\lfloor \frac{n-w+\delta}{\delta} \right\rfloor \cdots \right\rfloor \right\rfloor.$$

Proof. First observe that $A_2(n-w+\delta, 2\delta, \delta) = \left\lfloor \frac{n-w+\delta}{\delta} \right\rfloor$. This follows from the fact that codewords must have disjoint sets of 1's. Applying Theorem 1.1.38 iteratively $w-\delta$ times yields the bound of this corollary. □

Theorem 1.1.40.

$$A_2(n,d,w) \leqslant \left\lfloor \frac{n}{n-w} A_2(n-1,d,w) \right\rfloor$$

Proof. If we take the complement of an (n, M, d, w)-code, i.e. swithing the ones and zeros in the entries of the codewords, we obtain a code with the same length n, the same number of codewords M and the same distance distribution, but the weight will be $n-w$. Therefore, $A_2(n,d,w) = A_2(n,d,n-w)$. It follows from Theorem 1.1.38 that

$$A_2(n,d,n-w) \leqslant \left\lfloor \frac{n}{n-w} A_2(n-1,d,n-w-1) \right\rfloor.$$

But again, because of the observation about switching the ones and zeros, we have

$$A_2(n-1,d,n-w-1) = A_2(n-1,d,w),$$

which proves the theorem. □

1.1.4 Insertion-and-deletion correcting codes and the Levenshtein distance

In this subsection we introduce insertion-and-deletion correcting codes, based on [25]. These are codes where we can correct a certain combination of deletions of original symbols and insertions of new symbols in the codeword. We will also introduce a related distance function and give an analogon of Theorem 1.1.7.

Definition 1.1.41. (i) A code is ***e-deletion/insertion correcting*** if it is a code with the possibility to correct every combination of maximum e insertions and deletions.

(ii) An ***d-deletion i-insertion correcting code*** is a code which corrects every combination of at most d deletions and at most i insertions.

So, if a codeword c from an e-deletion/insertion correcting code is transmitted over some communication channel and if the received word r is obtained from c by a sequence of at most e deletions and insertions , then it is possible (at least in theory) to retrieve the original word c from r.

For the d-deletion i-insertion correcting code, the d and i are fixed and then if a codeword c is transmitted, we know that the received word r is obtained from c by a sequence of at most d deletions and at most i insertions, and so we can find the transmitted word c from r.

Notice that an e-deletion/insertion-correcting code is also a d-deletion i-insertion correcting code, $\forall d, i$ such that $d+i \leqslant e$. The reverse does not always hold, as you can see in the next example.

Example 1.1.42. Let $F_1 = \{0\}$ and $\mathcal{C} = \{0, 00000\}$. This code is not 2-deletion/insertion correcting, since the received word $y = 000$ could be a transformed word from the transmitted codeword $c_1 = 0$ by inserting two zeros or from the codeword $c_2 = 00000$ by deletion of two zeros. On the other hand, the code $\mathcal{C}$ is d-deletion i-insertion correcting if $d + i \leqslant 2$. For instance if $(d, i) = (0, 2)$ and we receive the word $y = 000$, then we know that the transmitted codeword is $c_2 = 00000$.

Definition 1.1.43. Let $(F_q)^*$ be the set of all words over F_q. Let $x = x_1 x_2 \dots x_n$ be a codeword over F_q of length n. A ***subsequence*** of x is a word in $(F_q)^*$

$$w = x_{i_1} x_{i_2} \dots x_{i_{|w|}}, \qquad 1 \leqslant i_1 < i_2 < \dots < i_{|w|} \leqslant n.$$

A word $w \in (F_q)^*$ is a ***common subsequence*** of the codewords $x, y \in (F_q)^*$ if w is a subsequence of both x and y. Note that x, y and w do not have to be of the same length. The length of the ***largest common subsequence*** of two words x and y in $(F_q)^*$ is denoted as $\boldsymbol{\rho(x, y)}$, i.e.

$$\rho(x, y) \coloneqq \max\{|w| | w \text{ is a common subsequence of } x \text{ and } y\}.$$

We will use this value ρ to define the distance for insertion-and-deletion correcting codes.

Definition 1.1.44. (i) The ***Levenshtein distance*** $\boldsymbol{\delta(x, y)}$ between two words x, y in $(F_q)^*$ is defined by

$$\delta(x, y) \coloneqq |x| + |y| - 2\rho(x, y). \tag{1.1.1}$$

(ii) The ***modified Levenshtein distance*** $\boldsymbol{\delta^*(x, y)}$ between two words $x, y \in (F_q)^*$ is defined by

$$\delta^*(x, y) \coloneqq ||x| - |y|| + \delta(x, y). \tag{1.1.2}$$

We can also write the modified Levenshtein distance as

$$\delta^*(x, y) \coloneqq 2 \max(|x| - \rho(x, y), |y| - \rho(x, y)).$$

This follows from the fact that, assuming that $|x| \geqslant |y|$,

$$\begin{aligned} \delta^*(x, y) &= |x| - |y| + |x| + |y| - 2\rho(x, y) \\ &= 2(|x| - \rho(x, y)) \\ &\geqslant 2(|y| - \rho(x, y)). \end{aligned}$$

The case $|x| \leqslant |y|$ can be shown analogously.

It can be easily shown (see e.g. [25]) that δ and δ^* are both metrics. These metrics will be used to define the minimum distances for the codes.

Definition 1.1.45. (i) The ***minimum Levenshtein distance*** $\boldsymbol{\delta(\mathcal{C})}$ of a code $\mathcal{C}$ is defined by

$$\delta(\mathcal{C}) \coloneqq \min_{x, x' \in \mathcal{C}; x \neq x'} \delta(x, x').$$

(ii) The ***minimum modified Levenshtein distance $\delta^*(\mathcal{C})$*** of $\mathcal{C}$ is defined by

$$\delta^*(\mathcal{C}) := \min_{x,x' \in \mathcal{C}; x \neq x'} \delta^*(x, x').$$

From the definitions it follows that $\delta(\mathcal{C}) \leqslant \delta^*(\mathcal{C})$.

In [25] the two following theorems are shown.

Theorem 1.1.46. *A code $\mathcal{C} \subseteq (F_q)^*$ is e-deletion/insertion correcting if and only if*

$$2e < \delta(\mathcal{C}).$$

Theorem 1.1.47. *A code $\mathcal{C} \subseteq (F_q)^*$ is d-deletion i-insertion correcting if and only if*

$$2(d+i) < \delta^*(\mathcal{C}).$$

From the definitions of δ and δ^* it follows that $\delta(x, y) = \delta^*(x, y)$ if x and y have the same length. This involves the next corollary.

Corollary 1.1.48. *A code $\mathcal{C} \subseteq (F_q)^n$, in which each codeword has the same length n, is d-deletion i-insertion correcting if and only if the code is $(d+i)$-deletion/insertion correcting.*

1.2 Designs

Definition 1.2.1. A ***t-(n, k, λ) design***, with $t, n, k, \lambda \in \mathbb{N}$, with[1] $n > k > 1, k \geqslant t \geqslant 1$, $\lambda > 0$, is an ordered triple $\mathcal{D} = (P, B, I)$, where P, called the set of ***points***, and B, called the set of ***blocks***, are finite sets and I an incidence relation such that

(i) $|P| = n$ and each element $L \in B$ is incident with exactly k elements of P,

(ii) each t different elements of P are incident with exactly λ common elements of B.

In other words, a t-(n, k, λ) design is a set X of n points and a collection of distinct k-subsets of X, i.e. subsets of X with k elements, called blocks, with the property that any t-subset of X is contained in exactly λ common blocks.

Example 1.2.2. Consider the m-dimensional projective space $\mathrm{PG}(d, q), d \geqslant 2$, over the finite field $\mathbb{F}_q$. Let P be the set of points of $\mathrm{PG}(d, q)$, B the set of the lines of $\mathrm{PG}(d, q)$ and I the natural incidence relation. Then $|P| = \frac{q^{d+1}-1}{q-1}$, the number of points incident with a block is $q+1$, and 2 different points define exactly one block. Consequently $\mathcal{D} = (P, B, I)$ is a 2-$(\frac{q^{d+1}-1}{q-1}, q+1, 1)$ design.

This example is a special case of a t-(n, k, λ) design with $\lambda = 1$, called a Steiner system.

[1] These conditions are only to exclude trivial cases.

Definition 1.2.3. A t-$(n, k, 1)$ design is a ***Steiner system*** $\mathcal{S}(t, k, n)$.

Or in other words, a Steiner system $\mathcal{S}(t, k, n)$ is a collection $\mathcal{S}$ of k-subsets, called blocks, of an n-set such that every t-subset of the n-set is contained in exactly one block of $\mathcal{S}$. Note that for a Steiner system we will use the notation $(X, \mathcal{S})$ or $\mathcal{S}$ if we do not need to specify the n-set X or if this ambient set X is clear from the context.

Definition 1.2.4. A ***t-(n, k, λ) covering design*** is a pair $(X, \mathcal{S})$, with X a set of n elements, called points, and $\mathcal{S}$ a set of k-subsets of X, called blocks, such that every subset of t points is contained in at least λ blocks of $\mathcal{S}$. The ***covering number $C_\lambda(n, k, t)$*** is the minimum number of blocks in a t-(n, k, λ) covering design.

The difference between a t-(n, k, λ) covering design and a t-(n, k, λ) design is manifested in the definitions in the important words 'at least' and 'exactly'.

Also for the case of t-(n, k, λ) covering designs, we consider the case where $\lambda = 1$.

Definition 1.2.5. We will define a t-$(n, k, 1)$ covering design by an ***(n, k, t)-covering design***. The minimum size of an (n, k, t)-covering design is the ***covering number $C(n, k, t) = C_1(n, k, t)$***. This covering design is a collection $\mathcal{S}$ of k-subsets of an n-set X such that every t-subset of elements of X is contained in at least one element of $\mathcal{S}$.

If a Steiner system $\mathcal{S}(t, k, n)$ exists, it is the smallest (n, k, t)-covering design. A relation between these concepts is shown in the next theorem, which is also a lower bound on $C(n, k, t)$.

Theorem 1.2.6. *Let $(X, \mathcal{S})$ be an (n, k, t)-covering design. Then*

$$|\mathcal{S}| \geqslant \frac{\binom{n}{t}}{\binom{k}{t}},$$

with equality if and only if $\mathcal{S}$ is a Steiner system $\mathcal{S}(t, k, n)$.

Proof. Every element of $\mathcal{S}$ is a k-subset of the ambient n-set X, and therefore contains exactly $\binom{k}{t}$ distinct t-subsets. Since the total number of t-subsets in X is $\binom{n}{t}$, we need at least $\frac{\binom{n}{t}}{\binom{k}{t}}$ elements in $\mathcal{S}$ to cover all these t-subsets, so $|\mathcal{S}| \geqslant \frac{\binom{n}{t}}{\binom{k}{t}}$. If $|\mathcal{S}|$ satisfies this bound with equality, each t-subset has to be contained in exactly one element of $\mathcal{S}$. This means that $(X, \mathcal{S})$ is a Steiner system $\mathcal{S}(t, k, n)$. And if $(X, \mathcal{S})$ is a Steiner system $\mathcal{S}(t, k, n)$, then the number of blocks of $\mathcal{S}$ is exactly $\frac{\binom{n}{t}}{\binom{k}{t}}$. □

Now we also present another lower bound for t-(n, k, λ) covering designs.

Theorem 1.2.7 (Schönheim bound)**.**

$$C_\lambda(n, k, t) \geqslant \left\lceil \frac{n}{k} \cdot C_\lambda(n-1, k-1, t-1) \right\rceil.$$

Proof. Consider $(X, \mathcal{S})$, an optimal t-(n, k, λ) covering design with $|\mathcal{S}| = C_\lambda(n, k, t)$. Since $|X| = n$ and since each block of $\mathcal{S}$ contains k elements, the average number of elements of $\mathcal{S}$ in which a fixed element of X is contained, is $\frac{|\mathcal{S}|k}{n}$. So there has to be an element $x \in X$ that is contained in at most $\frac{|\mathcal{S}|k}{n}$ elements of $\mathcal{S}$. Now define

$$X' \coloneqq X \backslash \{x\}$$

and

$$\mathcal{S}' \coloneqq \{S \backslash \{x\} \,|\, S \in \mathcal{S}, x \in S\}.$$

This construction implies that

$$|\mathcal{S}'| \leqslant \frac{k}{n} \cdot |\mathcal{S}| = \frac{k}{n} \cdot C_\lambda(n, k, t).$$

To prove the theorem, it remains to be shown that $(X', \mathcal{S}')$ is a $(t-1)$-$(n-1, k-1, \lambda)$ covering design, since, from the fact that $C_\lambda(n, k, t)$ is an integer, it follows that

$$\left\lceil \frac{n}{k} \cdot C_\lambda(n-1, k-1, t-1) \right\rceil \leqslant \left\lceil \frac{n}{k} \cdot |\mathcal{S}'| \right\rceil \leqslant C_\lambda(n, k, t).$$

First, the definitions of X' and $\mathcal{S}'$ imply that $|X'| = n-1$ and $|S| = k-1$ for all $S \in \mathcal{S}'$. Let A be an arbitrary subset of $t-1$ elements of X'. Therefore, the set $A \cup \{x\}$ is a subset of size t of X and hence, there exist at least λ blocks of $\mathcal{S}$, say $S_1, \ldots, S_\lambda$, containing $A \cup \{x\}$. These blocks S_i are also blocks of $\mathcal{S}'$, since they all contain x. Consequently, $S_1 \backslash \{x\}, \ldots, S_\lambda \backslash \{x\}$ are blocks of $\mathcal{S}'$ and do contain A. This means that A is contained in at least λ blocks of $\mathcal{S}'$ and so, $(X', \mathcal{S}')$ is a $(t-1)$-$(n-1, k-1, \lambda)$ covering design. □

For the special case of (n, k, t)-covering designs, this bound is

$$C(n, k, t) \geqslant \left\lceil \frac{n}{k} \cdot C(n-1, k-1, t-1) \right\rceil.$$

We will give an analogous bound for the case of q-covering designs in Theorem 4.4.14, with an analogous proof, and also the following corollary will be considered (see Corollary 4.4.15).

Corollary 1.2.8.

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

Proof. Applying Theorem 1.2.7 iteratively $t-1$ times for $\lambda = 1$ gives us

$$C(n, k, t) \geqslant \left\lceil \frac{n}{k} \left\lceil \frac{n-1}{k-1} \left\lceil \cdots \left\lceil \frac{n-t+2}{k-t+2} C(n-t+1, k-t+1, 1) \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

Observing that $C(n-t+1, k-t+1, 1) = \left\lceil \frac{n-t+1}{k-t+1} \right\rceil$, proves the corollary. □

We also mention the dual notion of an (n, k, t)-covering design.

Definition 1.2.9. An ***(n, k, t)-Turán design*** is a pair $(X, \mathcal{S})$, with X a set of n elements and $\mathcal{S}$ a set of t-subsets of X, called blocks, such that every subset S of k elements contains at least one block of $\mathcal{S}$. The ***Turán number $T(n, k, t)$*** is the minimum number of blocks in an (n, k, t)-Turán design.

The duality between these concepts is stated in the following theorem, shown in [39].

Theorem 1.2.10. *By taking the complement of each block of an (n, k, t)-Turán design, we obtain an $(n, n-t, n-k)$-covering design and vice versa. It also follows that*

$$T(n, k, t) = C(n, n-t, n-k).$$

To end this section, we want to show that it is natural that in this dissertation we have attention for both codes and designs. We can construct certain codes from designs, e.g. a binary constant-weight code can be constructed from a Steiner system.

Example 1.2.11. Let $\mathcal{S}$ be a Steiner system $\mathcal{S}(t, k, n)$. Now we construct a code of which the codewords correspond in the following way to the k-sets of $\mathcal{S}$. If $X = \{x_1, x_2, \ldots, x_n\}$ is the set of n points of this special design and K a k-subset of X, then the corresponding codeword is a vector of length n where the ith position is 1 if $x_i \in K$ and 0 if $x_i \notin K$. Since $|K| = k$, the weight of every vector is k. Since every t-subset of X is contained in exactly one element of $\mathcal{S}$, the intersection $y \cap z$ of two codewords y, z corresponding to two distinct blocks K_1, K_2, cannot have a weight larger than or equal to t. Indeed, otherwise the nonzero entries give rise to t elements which are contained in 2 blocks of the Steiner system. Therefore, $w(y \cap z) \leqslant t-1$ and, by Theorem 1.1.16,

$$d(y, z) = w(y) + w(z) - 2w(y \cap z) \geqslant 2(k - t + 1).$$

Now, if we can find two blocks with an intersection of size $t-1$, it follows that the code obtained from the Steiner system $\mathcal{S}(t, k, n)$ has minimum distance $2(k-t+1)$. For this purpose, fix a $(t-1)$-subset A, then there are still $n-t+1$ elements of X left. If we add an arbitrary point of $X \backslash A$ to the fixed set A, this gives a well defined t-subset T. This T is contained in exactly one block K. But if we construct all such t-sets in this way and consider the corresponding blocks of $\mathcal{S}$ in which the t-sets are contained, then every block K is counted $k-t+1$ times. Therefore, through a fixed $(t-1)$-subset there are $\frac{n-t+1}{k-t+1} \geqslant 2$ different blocks and so, there are at least two corresponding codewords with a minimum distance $2(k-t+1)$. Consequently, if you consider codewords which correspond to elements of a Steiner system $\mathcal{S}(t, k, n)$ as explained above, this is an (n, M, d, k)-code with $M = \frac{\binom{n}{t}}{\binom{k}{t}}$ and $d = 2(k-t+1)$.

1.3 Graph theory

In this section, we consider some basic notions of graph theory. The goal here is to introduce the Hamming graph and the Johnson graph. We do this by defining the notion of association schemes.

1.3.1 Some basic concepts

Definition 1.3.1. A ***graph $G = (V, E)$*** consists of a finite set V of ***vertices or nodes*** together with a set E of ***edges***, which are pairs of two vertices. Two vertices joined by an edge are called ***adjacent***.

Definition 1.3.2. An ***undirected*** graph G is a graph in which edges have no orientation. Opposite to this, a ***directed*** graph $G = (V, E)$ is a graph where E is a set of ordered pairs of vertices, and so, the edge (x, y) starts in x and has y as end vertex. If for a graph $G = (V, E)$ multiple edges between two vertices are allowed, we call this graph a ***multigraph***. A ***loop*** is an edge which starts and ends in the same vertex. If a graph G is undirected, has no loops and has no more than one edge between any two different vertices, this graph is called a ***simple graph***.

Definition 1.3.3. A ***complete graph*** is a graph of which each pair of vertices is joined by an edge.

In the following figure we give an example of a graph, typically visualised as a set of dots for the vertices, joined by lines for the edges. The graph is called the Petersen graph.

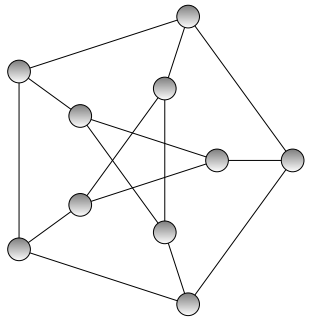


Figure 1.2: Petersen graph

Definition 1.3.4. A ***path*** in a graph G is a sequence of edges which connect a sequence of vertices. The ***graph distance*** $d(x, y)$ between two vertices x and y of a finite graph is the minimum length of the paths connecting them, i.e. the length of the shortest path between two vertices of a graph, the so called ***graph geodesic***. The longest shortest path of a graph is the ***graph diameter*** d, so $d := \max_{u,v \in G} d(u, v)$.

Definition 1.3.5. In an undirected graph G, two vertices are called ***connected*** if G contains a path from one to the other, otherwise they are called ***disconnected***. A graph is called connected if every pair of distinct vertices in the graph is connected, otherwise it is called disconnected.

Definition 1.3.6. The ***min-cut of a graph*** is the minimum number of edge deletions in the graph that would cause a partition of the vertices of a graph into two disjoint subsets which are not connected.

1.3.2 Association schemes and related graphs

Definition 1.3.7. A ***d-class association scheme*** on a finite set Ω is a pair $(\Omega, \mathcal{R})$ with $\mathcal{R}$ a set of symmetric relations $\{\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_d\}$ such that the following axioms hold:

(i) $\mathcal{R}_0 = \{(x, x) | x \in \Omega\}$ and is called the identity relation,

(ii) $\mathcal{R}$ is a partition of Ω^2,

(iii) there are ***intersection numbers*** p_{ij}^k such that for each $(x, y) \in \mathcal{R}_k$, the number of elements z in Ω for which $(x, z) \in \mathcal{R}_i$ and $(z, y) \in \mathcal{R}_j$ equals p_{ij}^k. This constant p_{ij}^k number only depends on i, j and k and not on the particular choice of x and y.

All the relations $\mathcal{R}_i$ are symmetric regular relations with valency p_{ii}^0.

If $(x, y) \in \mathcal{R}_i$, we call the two elements x and y ***ith associates***. So each element of Ω is its own zeroth associate while distinct elements are never zeroth associates. If x and y are kth associates, then the number of elements z which are both ith associates of x and jth associates of y, is a constant p_{ij}^k.

Definition 1.3.8. (i) The ***Johnson scheme***, denoted by $J(n, k)$, is defined as follows. Let Ω be a set with n elements. The elements of the scheme $J(n, k)$ are the $\binom{n}{k}$ subsets of Ω with k elements. Two k-subsets X and Y are ith associates when their intersection has size $k - i$.

(ii) The ***Hamming scheme***, denoted by $H(n, q)$, is defined as follows. The points of $H(n, q)$ are het q^n ordered n-tuples over a set of size q. Two n-tuples x and y are said to be ith associates if they disagree in exactly i coordinates.

We can interpret an association scheme as a complete graph with labelled edges. The vertices of the graph are the elements of Ω. The edge joining vertices x and y is labelled by i if $(x, y) \in \mathcal{R}_i$, so if x and y are ith associates. The loops of the graph are the edges labelled 0 at each vertex x, corresponding to $\mathcal{R}_0$. The interpretation of the intersection numbers is as follows. The number of triangles with a fixed base labelled k and having the other edges labelled i and j, is the constant number p_{ij}^k. Again, this constant does only depend on i, j, k and not on the choice of the base with label k. So for any vertices x and y of the graph and any integers $i, j = 0, 1, \ldots, d$ (where d is the graph diameter), the number of vertices at distance i from x and distance j from y depends only on i, j and the graph distance k between x and y, independent of the choice of x and y.

Furthermore each vertex is adjacent with exactly $v_i := p_{ii}^0$ edges labelled i.

A distance-regular graph is an example of a graph that constitutes an association schemes. Let G be a connected graph with diameter d on a set of vertices Ω. For every i in $\{0, \ldots d\}$ we let G_i denote the graph on the same set Ω, with two vertices adjacent if and only if they are at distance i in G, and we write $\mathcal{R}_i$ for the corresponding symmetric relation on Ω. The graph G is said to be distance-regular if the set of relations $\{\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_d\}$ induces an association scheme on Ω. In [6] it is shown that this is equivalent to the next definition.

Definition 1.3.9. A ***distance-regular graph*** G is a connected graph for which there exist integers b_i, c_i, $i = 0, \ldots, d$ (where d is the graph diameter) such that for any vertices $x, y \in G$ and distance $i = d(x, y)$ there are exactly c_i adjacent vertices of $y \in G_{i-1}(x)$ and b_i neighbours of $y \in G_{i+1}(x)$, where $G_i(x)$ denotes the set of vertices $y \in G$ with $d(x, y) = i$. Furthermore, the number of neighbours of y whose distance from x is i is denoted by a_i. The numbers a_i, b_i and c_i are called the intersection numbers and if k is the degree of any vertex, we have that $a_i + b_i + c_i = k$.

Complete graphs and the Petersen graph are examples of distance-regular graphs.

The definitions of the two specific association schemes in Definition 1.3.8 give rise to the following distance-regular graphs.

Definition 1.3.10. (i) The ***Johnson graph*** of the k-sets in Ω, with $|\Omega| = n$, has the collection of k-subsets of Ω as vertex set. Two vertices are adjacent whenever their intersection has size $k - 1$. Because of the close relation with the Johnson scheme, we also denote the related Johnson graph by $J(n, k)$. In Theorem 9.1.2 in [6], it is shown that this graph has diameter $d = \min(k, n - k)$, has $\binom{n}{k}$ vertices and is distance-transitive with intersection numbers

$$b_j = (k - j)(n - k - j) \text{ and } c_j = j^2 \quad (0 \leqslant j \leqslant d).$$

(ii) Let Ω be a set of size $q \geqslant 2$. The ***Hamming graph*** with diameter n on Ω is the graph with vertex set Ω^n, whereby two vertices are adjacent when they differ in one coordinate. The graph is denoted by $H(n, q)$, in the literature, the notation $L_q(n)$ is sometimes used. The Hamming graph has q^n vertices and is distance-regular with parameters

$$b_j = (d - j)(q - 1) \text{ and } c_j = j \quad (0 \leqslant j \leqslant n), \tag{1.3.1}$$

as we can find in [6]. The Hamming graph $H(n, q)$ is related to codes in the Hamming space $\mathcal{H}(n, q)$, as the name suggests, by taking the codewords of given length n as the vertices and where two codewords are adjacent if they differ in one position.

1.4 q-analogues

Definition 1.4.1. A ***q-analogue***, also called a q-extension or q-generalization, of a theorem, an identity or an expression is a generalization involving a new parameter q that returns the original theorem, identity or expression in the limit as $q \to 1$.

The basis for the q-analogues of the nonnegative integers is the equality

$$\lim_{q \to 1} \frac{q^n - 1}{q - 1} = n.$$

Definition 1.4.2. For a nonnegative integer n, the ***q*-analogue of *n***, also known as the q-bracket or q-number of n, is defined by

$$[n]_q = \frac{q^n - 1}{q - 1} = q^{n-1} + \ldots + q^2 + q + 1.$$

With this definition of $[n]_q$ we can define the q-analogue of the factorial, known as the q-factorial, by

$$\begin{aligned}[n]_q! &= [1]_q \cdot \cdots [n-1]_q \cdot [n]_q \\ &= \frac{q-1}{q-1} \cdot \frac{q^2-1}{q-1} \cdots \frac{q^{n-1}-1}{q-1} \cdot \frac{q^n-1}{q-1} \\ &= 1 \cdot (q+1) \cdots (q^{n-2} + \ldots + q + 1) \cdot (q^{n-1} + \ldots + q + 1).\end{aligned}$$

From the q-factorials, one can move on to define the q-binomial coefficients, also known as the q-ary Gaussian coefficients, Gaussian polynomials or Gaussian binomial coefficients.

Definition 1.4.3. The ***q*-ary Gaussian coefficient** is defined, for nonnegative integers k and n with $k \leqslant n$, by

$$\begin{aligned}\begin{bmatrix} n \\ k \end{bmatrix}_q &:= \frac{[n]_q!}{[n-k]_q![k]_q!} \\ &= \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)} \\ &= \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1},\end{aligned}$$

where the empty product, obtained when $k = 0$, is defined by 1.

It is well known (see e.g. Lemma 9.3.2 in [6]) that the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ gives the number of distinct k-dimensional subspaces of an n-dimensional vector space V over $\mathbb{F}_q$, since there are $\prod_{i=0}^{k-1}(q^n - q^i)$ ordered k-tuples of linearly independent vectors in V, and $\prod_{i=0}^{k-1}(q^k - q^i)$ ordered bases of any k-dimensional subspace. Even more, the number of subspaces of dimension k in an n-dimensional vector space V over $\mathbb{F}_q$, through a fixed subspace of dimension t is $\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$.

Letting q approach 1, we obtain the binomial coefficient $\binom{n}{k}$ or in other words, the number of k-element subsets of an n-element set.

Thus, one can regard a finite vector space as a q-generalization of a set, and the subspaces as the q-generalization of the subsets of the set. This interesting point of view has been the basis for a lot of related research. We give an example of the Erdős–Ko–Rado theorem and his q-analogue, mentioned in [12].

In 1961, Erdős, Ko and Rado published a theorem which gives a sharp upper bound on the size of the largest sets of pairwise non-trivially intersecting k-subsets of an n-set, the so-called Erdős-Ko-Rado sets ([16]). In the following theorem, we stated the improvement of this theorem by Wilson in 1984 in [41].

Theorem 1.4.4. *Let $1 \leqslant t \leqslant k$ be positive integers. If $\mathcal{S}$ is a family of subsets of size k in a set Ω with $|\Omega| = n$ and $n \geqslant (t+1)(k-t+1)$, such that the elements of $\mathcal{S}$ pairwise intersect in at least t elements, then*

$$|\mathcal{S}| \leqslant \binom{n-t}{k-t}.$$

If $n \geqslant (t+1)(k-t+1)+1$, then equality holds if and only if $\mathcal{S}$ is the set of all subsets of size k through a fixed t-subset of Ω.

Inspired by the results on Erdős-Ko-Rado sets, also the q-analogue results were introduced. These are the sets of k-dimensional subspaces in $V(n,q)$, the n-dimensional vector space over the finite field $\mathbb{F}_q$, $2k \leqslant n$, pairwise intersecting non-trivially. After hard work by researchers as Hsieh, Frankl and Wilson, the q-analogue of Theorem 1.4.4 was stated by Tanaka in [35].

Theorem 1.4.5. *Let $1 \leqslant t \leqslant k$ be positive integers. If $\mathcal{S}$ is a set of k-dimensional subspaces in $V(n,q)$, with $n \geqslant 2k$, pairwise intersecting in at least a t-dimensional subspace, then*

$$|\mathcal{S}| \leqslant \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q.$$

Furthermore, equality holds if and only if $\mathcal{S}$ is the set of all subspaces of dimension k, containing a fixed t-dimensional subspace of $V(n,q)$, or $n = 2k$ and $\mathcal{S}$ is the set of all subspaces of dimension k in a fixed $(n-t)$-dimensional subspace.

In these theorems, we can indeed see the analogy between the binomial coefficients and the Gaussian coefficients, and the analogy between the subsets of a set and the subspaces of a vector space over a finite field.

Also in coding theory we can give q-generalizations of certain theorems. One of the goals of this dissertation is to give q-analogues of different concepts. For instance, in Chapter 2 we introduce the Grassmann graph, which is the q-analogue of the Johnson graph. In Chapter 3 we give some bounds in the Hamming space which are the q-analogues of bounds in Subsection 1.1.3, even some proofs are similar. Also designs and spreads will be handled for this purpose.

Chapter 2

Coding for errors and erasures in random network coding

2.1 Random network coding

2.1.1 General idea

Like many fundamental concepts, network coding is based on a simple basic idea which was first stated in the paper [2] by R. Ahlswede et al., as noticed in [1].

Simply represented, a ***network*** is a directed multigraph which consists of different nodes. As you can see in figure 2.1 ([37]), the source nodes transmit messages to the sink nodes through a channel of inner nodes, also known as the intermediate network nodes. The core notion of network coding is to allow and encourage mixing of data at these intermediate network nodes. A receiver sees the data packets and deduces from them the messages that were originally intended for the sinks. In contrast to traditional ways to operate a network that tries to avoid collisions of data streams as much as possible, one of the most interesting opportunities of this approach is just the use of random mixing of data streams.

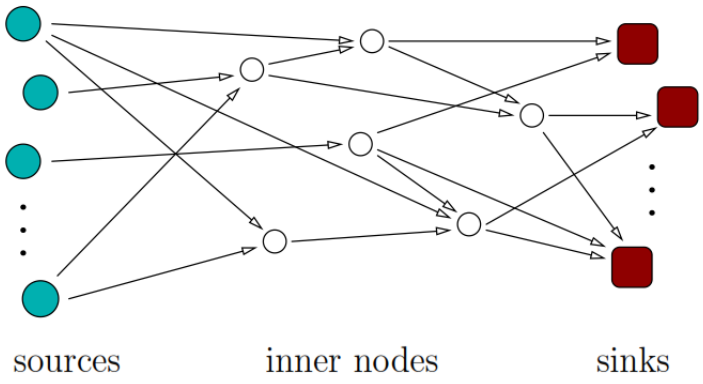


Figure 2.1: A network with source, inner and sink nodes

The article of Kötter and Kschischang ([28]) has given the interest in random network coding an enormous boost. This article is also the basis of this chapter.

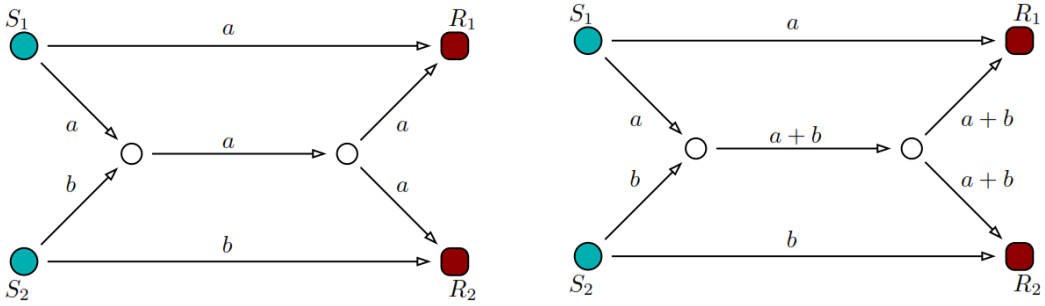
The principle of network coding is easiest explained with an example (see e.g. [2]), called the butterfly network. Some people say that every talk about random network coding has to include the example of the butterfly network, so we will also follow this approach.

2.1.2 Butterfly network

In this example two sources have access to information a and b at a rate of one bit per unit time. They have to communicate these to the two sink nodes, which each want to know both a and b per unit time. The sources send a and b to the first intermediate node. All links have a capacity of one bit per unit time, so each edge can carry only a single value.

If only forwarding were allowed, then the central link would be only able to carry a or b, but not both. If we would send a through the center, then the upper receiver R_1 would receive a twice and not know b at all. Suppose we send b to the center, it poses a similar problem for the lower receiver R_2. This situation is visualised in figure 2.2a ([37]).

By sending the sum of a and b through the center, a and b can be transmitted to both destinations simultaneously, as shown in figure 2.2b. The upper sink node receives a and $a + b$, and can calculate b by subtracting the two values. Similarly, the lower sink will receive b and $a + b$, and will also be able to determine both a and b.



(a) Only forwarding **(b)** Butterfly network

Figure 2.2

2.1.3 Random linear network coding

Random network coding uses the same idea as the butterfly network. When sending information through a network, we can optimize the throughput by doing linear combinations on the intermediate nodes. We call it ***linear network coding***.

According to [28], the standard, widely advocated approach to random linear network coding is as follows. The source(s) randomly choose(s) the parameters of all inner nodes

beforehand and send(s) these as 'headers' of the information packets. These headers are used to decode the codewords, which are rank-metric codes.

In contrast, in this thesis we consider a 'noncoherent' or 'channel oblivious' model, where neither transmitter nor receiver is assumed to have knowledge of the channel transfer characteristic. That means that the inner nodes transmit a random linear combination of the incoming information, but the parameters are not known in general. So if the source nodes send some vectors in the model, we receive in the sink nodes some vectors which are linear combinations of the transmitted vectors. Because the model is 'memoryless', we cannot deduce from the received information the original vectors. That is why here the codewords will not be vectors, but vector spaces, conveyed via transmission of a generating set for that space.

From [28] we know that the communication between transmitter and receiver occurs in a series of rounds or 'generations'. During each generation, the transmitter sends a number of packets of a fixed length into the network. Each packet may be seen as a row vector of length n over a finite field $\mathbb{F}_q$. Through the network, these packets possibly pass through a number of intermediate nodes. Whenever an intermediate node has an opportunity to send a packet, it creates a random $\mathbb{F}_q$-linear combination of the packets it received and transmits this. Finally, the receiver collects such randomly generated packets and tries to deduce the set of packets which the source has injected into the network.

2.1.4 Errors and erasures

Random network coding is a powerful tool for transmitting information in networks, yet it is susceptible to errors and erasures.

Definition 2.1.1. ***Errors*** are erroneously received packets and ***erasures*** insufficiently many received packets.

Packet transmission errors can be caused by noise or intentional jamming. In Subsection 2.1.5, it will be shown that, even a single error in one received packet can make the entire transmission useless when the erroneous packet is combined with other received packets to deduce the transmitted information. Another problem of deducing the transmitted message can happen when insufficiently many packets from one generation reach the receivers.

If we take the set of successful packet transmissions in a generation, this induces a directed multigraph with the same vertex set as the network and where the edges denote successful packet transmissions. The rate of information transmission (packets per generation) between the transmitter and the receiver is upper-bounded by the min-cut (see Definition 1.3.5) between these nodes. Random network coding in $\mathbb{F}_q$ is able to achieve a transmission rate that reaches the min-cut with probability approaching one as $q \to \infty$, as shown in [24].

In the next sections, we formulate a coding theory that captures the effects of both errors and erasures.

2.1.5 Operator channel

We will now introduce a concise and convenient abstraction of the channel encountered in random linear network coding, when neither transmitter nor receiver have knowledge of the channel transfer characteristics.

We will formulate our problem for the case of a unicast, a communication between a single transmitter and a single receiver. See [24] for a generalization to multicasting.

Let $\{x_1, x_2, \ldots, x_m\}, x_i \in \mathbb{F}_q^n, i = 1, \ldots, m$, denote the set of the vectors transmitted by the source. In the error-free case, the receiver collects packets $y_j, j = 1, \ldots, l$, where each y_j is formed as a linear combination of the vectors x_i. So

$$y_j = \sum_{i=1}^{m} h_{ji} x_i$$

with unknown, randomly chosen coefficients $h_{ji} \in \mathbb{F}_q$.

Normally the receiver would collect as many packets as possible, so note that a priori the parameter l is not fixed. But there are properties, such as the min-cut between the transmitter and the receiver, who may influence the coefficients h_{ji}. So at some point, collecting further redundant information will give no benefit anymore.

Consider now the case where also t erroneous packets are injected. This model is enlarged with error packets $e_k, k = 1, \ldots, t$, so each received packet can be seen as

$$y_j = \sum_{i=1}^{m} h_{ji} x_i + \sum_{k=1}^{t} g_{jk} e_k$$

where again h_{ji} and g_{jk} are unknown random coefficients in $\mathbb{F}_q$.

Note that since these erroneous vectors may be injected anywhere within the network, they have the potential to cause widespread error propagation. In particular, a single error in one received packet can make the entire transmission useless. For example, if $g_{j1} \neq 0, \forall j$, even a single error packet e_1 may corrupt each and every received packet.

The transmission model can be written in matrix form as

$$y = Hx + Ge$$

where H and G are random $(l \times m)$- and $(l \times t)$-matrices, respectively, x is the $(m \times n)$-matrix whose rows are the transmitted vectors, y is the $(l \times n)$-matrix whose rows are the received vectors, and e is the $t \times n$ matrix whose rows are the error vectors.

Since H is a random matrix, the question arises what property of the injected sequence of packets remains invariant in the transmission model explained in this section, even in the error-free case where $e = 0$. The only thing that is fixed by the product Hx, when H is random, is the row space of x. Again, we see that we will not consider the rows of x, i.e. the transmitted vectors x_i, but the vector space spanned by these vectors. This observation is very important for the channel models and transmission strategies considered in this dissertation. With regard to the injected vector space, the only deleterious effect that a multiplication with H may have is that Hx may have

smaller rank than x. That can be attributed to an insufficient min-cut or packet erasures, for example. Then Hx will generate a subspace of the row space of x, and the rank corresponds to the dimension of the subspace.

Let $\mathcal{W}$ be an arbitrary fixed n-dimensional vector space over $\mathbb{F}_q$. All transmitted and received packets will be vectors of $\mathcal{W}$. However, we will describe a transmission model in terms of subspaces of $\mathcal{W}$ spanned by these packets. Let $\mathcal{P}(\mathcal{W})$ denote the set of all subspaces of $\mathcal{W}$, called the power set of $\mathcal{W}$. Since $\mathcal{W}$ is isomorphic to $\mathbb{F}_q^n$, we can see $\mathcal{P}(\mathcal{W})$ just as $\mathcal{P}(\mathbb{F}_q^n)$. This is the reason why we call the set of all subspaces of $\mathcal{W}$, including $\{0\}$ and $\mathcal{W}$ itself, the ***projective space*** of dimension $n-1$ over $\mathbb{F}_q$, associated with $\mathcal{W}$. In what follows, we will denote this by $\mathcal{P}_q(n)$.[1] Furthermore, in the following we assume that the dimensions are dimensions of vector spaces, unless stated otherwise, and subspaces of dimension k will sometimes be briefly called k-subspaces.

We denote $U+V=\{u+v|u\in U, v\in V\}$ as the sum of two subspaces $U,V\in\mathcal{P}_q(n)$. If $U\cap V=\{0\}$, then the sum $U+V$ is a direct sum, denoted as $U\oplus V$. It is clear that $\dim(U\oplus V)=\dim(U)+\dim(V)$. Furthermore, for any subspaces U and V we have $V=(U\cap V)\oplus V'$ for some subspace V' isomorphic to the quotient space $V/(U\cap V)$. So we can always transform a sum into a direct sum as follows

$$U+V=U+((U\cap V)\oplus V')=U\oplus V'.$$

Definition 2.1.2. For an integer $k\geqslant 0$, we define a stochastic operator $\boldsymbol{\mathcal{H}_k}$, called an ***erasure operator*** that operates on the subspaces of $\mathcal{W}$ as follows. If $\dim(V)\leqslant k$, $\mathcal{H}_k(V)=V$. If $\dim(V)>k$, then $\mathcal{H}_k(V)$ returns a randomly chosen k-dimensional supspace of $\mathcal{V}$.[2]

Let U and V be two subspaces of $\mathcal{W}$, it is always possible to realize U as $U=\mathcal{H}_k(V)\oplus E$ for some subspace E of $\mathcal{W}$, with $k=\dim(U\cap V)$ and $\mathcal{H}_k(V)=U\cap V$. This is the key to define the following 'operator channel' as a concise and convenient transmission model for random network coding.

Definition 2.1.3. An ***operator channel*** C associated with the ambient space $\mathcal{W}$ is a channel with input and output alphabet $\mathcal{P}(\mathcal{W})$. The channel input V and channel output U can always be related as

$$U=\mathcal{H}_k(V)\oplus E$$

with $k=\dim(U\cap V)$ and E an error space. In transforming V to U, we commit $\boldsymbol{\rho=\dim(V)-k}$ ***erasures*** and $\boldsymbol{t=\dim(E)}$ ***errors***.

Remark 2.1.4. We will note in Remark 2.2.11 that instead of the terminology 'erasures' and 'errors', it might be better to use the terminology 'deletions' and 'insertions' since there, we will be able to make a link between the metric defined in Subsection 2.2.1 and the Levenshtein metric for insertion-and-deletion correcting codes, discussed in Subsection 1.1.4.

[1] We will use the notations of [17]. This paper also includes the following remark. Many relevant papers, such as [28], refer to $\mathcal{P}_q(n)$ or $\mathcal{P}(\mathcal{W})$ as the projective geometry of $\mathcal{W}$. The terms 'projective geometry' and 'projective space' seem to be equally well-established in the literature. We feel that 'projective space' is more fortunate terminology, since $\mathcal{P}_q(n)$ is the ambient 'space' for the codes at hand.

[2] For the purposes of this thesis, the distribution of $\mathcal{H}_k(V)$ is unimportant.

Remark 2.1.5. We have chosen to model the error space E so that it intersects trivially with the transmitted subspace V, thus the choice of E is not independent of V. However, we can do that without loss of generality. Indeed, if we would model the received space as $U = \mathcal{H}_k(V) + E$ for an arbitrary error space E, then since E always decomposes for some space E' as $E = (E \cap V) \oplus E'$, we would get $U = \mathcal{H}_k(V) + (E \cap V) \oplus E' = \mathcal{H}_{k'}(V) \oplus E'$ for some $k' \geqslant k$. This means that the components of an error space E that intersects with the transmitted space V would only be helpful, possibly decreasing the number of erasures seen by the receiver.

2.2 Coding for operator channels

In summary, an operator channel takes in a vector space and puts out another vector space, possibly with erasures, i.e. deletion of vectors from the transmitted space, or errors, i.e. addition of vectors to the transmitted space.

In this section we will define a suitable metric, define some basic concepts, show how to construct codes that correct combinations of errors and erasures ... for this channel.

Recall that $\mathcal{W}$ is the fixed n-dimensional vector space over $\mathbb{F}_q$ and $\mathcal{P}_q(n)$ is the set of all subspaces of $\mathcal{W}$.

2.2.1 Metric

Definition 2.2.1. Let $\mathbb{Z}_+$ denote the set of nonnegative integers. We define the ***subspace distance*** $d : \mathcal{P}_q(n) \times \mathcal{P}_q(n) \to \mathbb{Z}_+$ by

$$d(U, V) \coloneqq \dim(U + V) - \dim(U \cap V). \tag{2.2.1}$$

The motivation of the choice of the metric follows from the insertions and deletions which occur by the transmission of information by random network coding.

Because $\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$, we may also write

$$\begin{aligned} d(U, V) &= \dim(U) + \dim(V) - 2\dim(U \cap V) \\ &= 2\dim(U + V) - \dim(U) - \dim(V). \end{aligned} \tag{2.2.2}$$

To be able to talk about distances between codewords, this function d needs to be a metric. This is indeed true, as is shown in the next lemma. We will call this metric the ***subspace metric***.

Lemma 2.2.2. *The function $d : \mathcal{P}_q(n) \times \mathcal{P}_q(n) \to \mathbb{Z}_+$ with*

$$d(U, V) \coloneqq \dim(U + V) - \dim(U \cap V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

is a metric for the space $\mathcal{P}_q(n)$.

Proof. Let $U, V, X \in \mathcal{P}_q(n)$. It is clear that the following two conditions are correct.

(i) $d(U,V) \geqslant 0$ and equality holds if and only if $U = V$.

(ii) $d(U,V) = d(V,U)$

So we just have to prove the triangle inequality,

(iii) $d(U,V) \leqslant d(U,X) + d(X,V)$.

This inequality holds because we have

$$\begin{aligned}
&d(U,V) - d(U,X) - d(X,V) \\
&\quad = \dim(U) + \dim(V) - 2\dim(U \cap V) - \dim(U) - \dim(X) + 2\dim(U \cap X) \\
&\qquad - \dim(X) - \dim(V) + 2\dim(X \cap V) \\
&\quad = 2(\dim(U \cap X) + \dim(V \cap X) - \dim(X) - \dim(U \cap V)) \\
&\quad = 2(\underbrace{\dim((U \cap X) + (V \cap X)) - \dim(X)}_{\leqslant 0} + \underbrace{\dim(U \cap V \cap X) - \dim(U \cap V)}_{\leqslant 0}) \qquad (2.2.3) \\
&\quad \leqslant 0.
\end{aligned}$$

The first inequality in (2.2.3) holds since $(U \cap X) + (V \cap X) \subseteq X$. Because of the property $U \cap V \cap X \subseteq U \cap V$, we also get the second inequality in (2.2.3).

By checking the three conditions we have obtained that d is a metric. □

Given a subspace U of $\mathcal{W}$ of dimension k, the orthogonal subspace of U in $\mathcal{W}$ is the $(n-k)$-dimensional subspace

$$U^{\perp} = \{v \in \mathcal{W} | u \cdot v = 0,\ \forall u \in U\},$$

where $u \cdot v$ is the standard inproduct of u and v.

For any subspaces U and V in $\mathcal{P}_q(n)$, the well known properties $(U^{\perp})^{\perp} = U$, $(U+V)^{\perp} = U^{\perp} \cap V^{\perp}$ and $(U \cap V)^{\perp} = U^{\perp} + V^{\perp}$ give a link between the distance between these subspaces and the distance between their orthogonal subspaces for this metric. Namely, the distances are perfectly mirrored, since it follows that

$$\begin{aligned}
d(U^{\perp}, V^{\perp}) &= \dim(U^{\perp} + V^{\perp}) - \dim(U^{\perp} \cap V^{\perp}) \\
&= \dim((U \cap V)^{\perp}) - \dim((U+V)^{\perp}) \\
&= (n - \dim(U \cap V)) - (n - \dim(U+V)) \qquad (2.2.4) \\
&= \dim(U+V) - \dim(U \cap V) \\
&= d(U,V).
\end{aligned}$$

2.2.2 Codes

Definition 2.2.3. A ***code*** for an operator channel with ambient space $\mathcal{W}$ is a nonempty subset of $\mathcal{P}_q(n)$, i.e. a nonempty collection of subspaces of $\mathcal{W}$.

With the subspace metric we can associate a notion of distance between codewords. An important concept in this context is the next definition.

Definition 2.2.4. The ***minimum distance*** of $\mathcal{C}$ is defined by

$$d(\mathcal{C}) \coloneqq \min_{U,V\in\mathcal{C}:U\neq V} d(U,V).$$

We often denote the minimum distance by d, if there is no possibility of ambiguity.

If we define the minimum distance d as above, denote the size of the code by $M = |\mathcal{C}|$ and if $d(U,V) \geqslant d$ for all different subspaces $U, V \in \mathcal{C}$ and there exist codewords U and V such that $d(U,V) = d$, then we say that $\mathcal{C}$ is an ***(n, M, d)-code in projective space***.

Definition 2.2.5. The ***complementary code*** corresponding to a code $\mathcal{C}$ is the code $\mathcal{C}^\perp = \{U^\perp | U \in \mathcal{C}\}$ obtained from the orthogonal subspaces of the codewords of $\mathcal{C}$.

Because $d(U^\perp, V^\perp) = d(U,V)$, as shown in (2.2.4), the minimum distance of the complementary code $\mathcal{C}^\perp$ is $d(\mathcal{C}^\perp) = d(\mathcal{C})$. If $\mathcal{C}$ is an (n, M, d)-code, then so is $\mathcal{C}^\perp$.

In the next subsection, we discuss an important group of codes, the constant-dimension codes.

2.2.3 Constant-dimension codes

Definition 2.2.6. A ***constant-dimension code*** is a code of which each codeword has the same dimension.

In the context of constant-dimension codes, it is natural to start with the following definition.

Definition 2.2.7. Given a nonnegative integer $k \leqslant n$, the set of all subspaces of $\mathcal{W}$ with dimension k is known as the ***Grassmannian*** $\mathcal{G}_q(n,k)$.

If an (n, M, d)-code $\mathcal{C}$ is contained in $\mathcal{G}_q(n,k)$ for some $k \leqslant n$, it is a constant-dimension code. In that case we say that $\mathcal{C}$ is an ***(n, M, d, k)-code***. Since $\forall U, V \in \mathcal{G}_q(n,k)$ it follows that $\dim(U) = \dim(V) = k$ and

$$d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V) = 2(k - \dim(U \cap V)),$$

so the distance between two codewords is always even and the minimum distance is at least 2.

Since $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, it follows that $M \leqslant |\mathcal{G}_q(n,k)|$. To determine the size of the Grassmannian $\mathcal{G}_q(n,k)$, we make use of the q-analogue of the binomial coefficient. In Section 1.4 we defined the q-ary Gaussian coefficient, for nonnegative integers k and n with $k \leqslant n$, by

$$\begin{aligned}\begin{bmatrix} n \\ k \end{bmatrix}_q &:= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} \\ &= \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1},\end{aligned}$$

where the empty product obtained when $k = 0$, is defined by 1.

Note that $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$. If it is clear that we work over $\mathbb{F}_q$, the Gaussian coefficient is sometimes denoted by $\begin{bmatrix} n \\ k \end{bmatrix}$, so without the index q.

We also noted (see Section 1.4) that the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ gives the number of distinct k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$. That is why the size of the Grassmannian $\mathcal{G}_q(n,k)$ is

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

If $\mathcal{C}$ is an (n, M, d, k)-code, $\mathcal{C}^\perp$ is a constant-dimension code of type $(n, M, d, n-k)$. So if we consider constant-dimension codes, we may restrict ourselves to (n, M, d, k)-codes with $k \leqslant \frac{n}{2}$, since a code of type (n, M, d, k) with $k > \frac{n}{2}$ may be replaced by its complementary code $\mathcal{C}^\perp$.

The (n, M, d, k)-codes are akin to constant-weight codes in the Hamming space. As these constant-weight codes correspond to a distance-regular Johnson graph, so does the metric space $\mathcal{G}_q(n,k)$ correspond to a distance-regular graph, called the Grassmann graph.

Definition 2.2.8. The ***Grassmann graph $G_q(n,k)$*** is a graph of which the vertex set is the set $\mathcal{G}_q(n,k)$ of all k-dimensional subspaces of $\mathcal{P}_q(n)$, and two vertices are adjacent if the corresponding subspaces intersect in a subspace of dimension $k-1$. So there is an edge joining vertices U and V if and only if $d(U,V) = 2$.

We also note that the distance between two subspaces $U, V \in \mathcal{G}_q(n,k)$ with the metric introduced in Definition 2.2.1, is an even number equal to twice the graph distance in the Grassmann graph.

In Theorem 9.3.3 in [6] it is shown that $G_q(n,k)$ has diameter $d = \min(k, n-k)$ and that $G_q(n,k)$ is distance transitive with intersection numbers

$$b_j = q^{2j+1}\begin{bmatrix} k-j \\ 1 \end{bmatrix}\begin{bmatrix} n-k-j \\ 1 \end{bmatrix} \text{ and } c_j = \begin{bmatrix} j \\ 1 \end{bmatrix}^2 \quad (0 \leqslant j \leqslant d), \tag{2.2.5}$$

so $G_q(n,k)$ is a distance-regular graph and constitutes an association scheme with relations given by the distance between spaces. The parameters in (2.2.5) are just the q-analogues of the intersection numbers of the Johnson graph. Because of the q-analogy

with the Johnson graph, the Grassmann graph is also called a q-Johnson graph. As such, techniques for bounds in the Hamming association scheme can be applied. In particular, sphere-packing and sphere-covering concepts have a natural equivalent formulation. We explore this in the next chapter.

Remark 2.2.9. Although we can link the codes in projective space with familiar codes in the Hamming space and codes contained in a Grassmannian with constant-weight codes in the Johnson space, there are important differences. We have seen that the Grassmannian $\mathcal{G}_q(n,k)$ corresponds to a distance-regular graph, similar to the distance-regular graph resulting from the Johnson space. But on the other hand, while the Hamming space $\mathbb{F}_q^n$ is always distance-regular as a graph, the graph associated with $\mathcal{P}_q(n)$ is not. We can define this graph as the graph with the elements of the projective space $\mathcal{P}_q(n)$ as vertices and two vertices are adjacent if and only if for the corresponding elements $A, B \in \mathcal{P}_q(n)$ $d(A,B) = \dim(A+B) - \dim(A \cap B) = 1$. For instance, from a projective view considered, the elements at distance 1 from a given point p in $\mathcal{P}_q(4)$ are the empty set and the q^2+q+1 lines through p. On the other hand, the elements at distance 1 from a given line L in $\mathcal{P}_q(4)$ are the $q+1$ points on L and the $q+1$ planes through L. So two spheres of the same radius in $\mathcal{P}_q(n)$ (see Definition 3.2.1) may have different sizes. This implies that conventional geometric intuition does not always apply.

2.2.4 Error and erasure correction

To conclude this chapter, we will give an important theorem which shows that codes in $\mathcal{P}_q(n)$ are precisely what is needed for error-correction in networks.

Recall that a minimum-distance decoder for a code $\mathcal{C}$ returns the nearest codeword for a given output. If U is the output of an operator channel, the minimum-distance decoder returns a codeword $V \in \mathcal{C}$ satisfying

$$d(U,V) \leqslant d(U,V'),\ \forall V' \in \mathcal{C}.$$

The next theorem shows us the error and erasure correction capability of a code $\mathcal{C}$ under minimum-distance decoding.

Theorem 2.2.10. *Let $\mathcal{C}$ be a code for transmission over an operator channel, $V \in \mathcal{C}$ be transmitted and*

$$U = \mathcal{H}_k(V) \oplus E$$

be received, where $\mathcal{H}_k$ is defined as in Definition 2.1.2 and $\dim(E) = t$. Let us denote the maximum number of erasures induced by the channel by $\rho = \max(0, \max_{U \in \mathcal{C}} \dim(U) - k)$. If

$$2(t+\rho) < d(\mathcal{C}), \tag{2.2.6}$$

then a minimum-distance decoder for $\mathcal{C}$ will return the transmitted codeword V from the received space U.

Proof. Let $V' = \mathcal{H}_k(V)$. The triangle inequality gives us

$$d(V,U) \leqslant d(V,V') + d(V',U) \leqslant \rho + t. \tag{2.2.7}$$

If $T \neq V$ is any other codeword in $\mathcal{C}$, then, again from the triangle inequality,

$$d(\mathcal{C}) \leqslant d(V,T) \leqslant d(V,U) + d(U,T).$$

From this inequality it follows that

$$d(U,T) \geqslant d(\mathcal{C}) - d(V,U).$$

By combining (2.2.7) and (2.2.6), we get

$$d(U,T) \geqslant d(\mathcal{C}) - (\rho + t) > \rho + t \geqslant d(U,V).$$

So a minimum-distance decoder must produce V, because V is the nearest codeword for U. □

Remark 2.2.11. As seen in the previous theorem, erasures and errors are equally costly to the decoder. This is in apparent contrast with traditional error-correction. Then an (n, M, d)-code can correct up to e errors and f erasures if $2e + f < d$, where an error is an incorrect value in an unknown position and an erasure is a position without a value, so a blank position. Indeed, if we receive a vector y with f blank positions which differs in $e + f$ positions from the transmitted codeword x and if x' is a codeword that differs $e' + f$ positions from y, with $e' \leqslant e$, then $d(x, x') \leqslant e + f + e' \leqslant 2e + f < d$. This shows that in this context erasures cost less than errors. However, this is rather a difference because of the terminology.

Perhaps more closely related classical concepts are 'deletions' and 'insertions', since in our situation of an operator channel associated with the ambient space $\mathcal{W}$, the erasures are deletions of dimensions and errors are insertions of dimensions. In Subsection 1.1.4, a code is called d-deletion i-insertion correcting if it is possible to correct every combination of at most d deletions and at most i insertions. There is a clear similarity between the Levenshtein distance for these codes ((1.1.1)) and the subspace distance for error-correcting codes in projective space ((2.2.2)). In Theorem 1.1.47 and the previous Theorem 2.2.10 you can see that also the capacity of correcting is similar, where the dimension t of the error space corresponds to the i insertions and the ρ erasures to the d deletions.

If we can be sure that the channel always returns at least the transmitted subspace, there are no erasures. This can be expressed by choosing operator $\mathcal{H}_{\dim(\mathcal{W})}$ which operates as an identity on each subspace of $\mathcal{W}$. This special case gives us the following corollary of Theorem 2.2.10.

Corollary 2.2.12. *Let $\mathcal{C}$ be a code for transmission over an operator channel, $V \in \mathcal{C}$ be transmitted and*

$$U = \mathcal{H}_{\dim(\mathcal{W})}(V) \oplus E = V \oplus E$$

be received, where $\dim(E) = t$. *If*

$$2t < d(\mathcal{C}), \tag{2.2.8}$$

then a minimum-distance decoder for $\mathcal{C}$ will produce V.

In other words, in the absence of erasures, a minimum-distance decoder uniquely corrects errors up to dimension

$$t \leqslant \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor .$$

This is in parallel to the standard error-correction situation, see Theorem 1.1.7.

Symmetrically, we consider the case where the network produces no errors, this means that the error space $E = \{0\}$. So we get the next corollary.

Corollary 2.2.13. *Let $\mathcal{C}$ be a code for transmission over an operator channel, $V \in \mathcal{C}$ be transmitted and*

$$U = \mathcal{H}_k(V) \oplus \{0\} = \mathcal{H}_k(V)$$

be received. If

$$2\rho < d(\mathcal{C}), \tag{2.2.9}$$

where $\rho = \max(0, \max_{U \in \mathcal{C}} \dim(U) - k)$, then a minimum-distance decoder for $\mathcal{C}$ will produce V.

Chapter 3

Bounds on codes in random network coding

The ***main coding theory problem*** is to construct 'good' codes, i.e. codes having a small length n, a large minimum distance d and a large number of codewords M. As in classical coding theory, we want to maximize the number of codewords for a given dimension n of an ambient space $\mathcal{W}$ and minimum distance d.

Definition 3.0.14. The largest value of M such that there exists an (n, M, d)-code in $\mathcal{P}_q(n)$ is denoted by $\mathcal{A}_q(n, d)$. The maximum number of codewords in an (n, M, d, k)-code in $\mathcal{G}_q(n, k)$ is denoted by $\mathcal{A}_q(n, d, k)$.

In order to find $\mathcal{A}_q(n, d)$ and $\mathcal{A}_q(n, d, k)$ for specific q, n, d, k, we will discuss bounds on these values, based on the articles [28] and [17]. First, we will discuss the bounds in the special case of constant-dimension codes.

3.1 Bounds on constant-dimension codes

3.1.1 Sphere-packing bound and sphere-covering bound

As we remarked earlier, the Grassmann graph constitutes an association scheme, which lets us use simple geometric arguments to give the standard sphere-packing upper bound and sphere-covering lower bound. In order to establish these bounds we need the notion of a sphere.

Definition 3.1.1. Let $V \in \mathcal{G}_q(n, k)$ be a subspace of the ambient n-dimensional vector space $\mathcal{W}$. The ***sphere*** $\boldsymbol{\mathcal{S}(V, k, r)}$ of radius r centered at a space V in $\mathcal{G}_q(n, k)$ is defined by

$$\mathcal{S}(V, k, r) \coloneqq \{U \in \mathcal{G}_q(n, k) | d(U, V) \leqslant 2r\}.$$

Note that the radius is defined in terms of the graph distance in the Grassmann graph. Since the distance between two elements in the Grassmannian $\mathcal{G}_q(n, k)$ is always even, this definition gives no restrictions.

Since $\mathcal{G}_q(n,k)$ constitutes a distance-regular graph, hence an association scheme, the number of spaces in $\mathcal{S}(V,k,r)$ is independent of V. This follows from the fact that in the Grassmann graph $G_q(n,k)$ the number of elements at graph distance $i \leqslant r$, i.e. $\sum_{i=0}^{r} p_{ii}^0$, is independent of the vertices. Therefore, if we don't want to specify the center of the sphere of radius r in $\mathcal{G}_q(n,k)$, we write $\boldsymbol{\mathcal{S}(n,k,r)}$.

Lemma 3.1.2. *The number of spaces in $\mathcal{S}(V,k,t)$ for $V \in \mathcal{G}_q(n,k)$ equals*

$$|\mathcal{S}(n,k,t)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix},$$

for $t \leqslant k$.

Proof. Since $d(U,V) = 2(k - \dim(U \cap V))$, for some $U, V \in \mathcal{G}_q(n,k)$, we first give an expression for the subspaces U that intersect V in a $(k-i)$-dimensional subspace, for some i, $0 \leqslant i \leqslant t$. We can choose the $(k-i)$-dimensional subspace of intersection in $\begin{bmatrix} k \\ k-i \end{bmatrix} = \begin{bmatrix} k \\ i \end{bmatrix}$ ways. To complete the subspace we take i linearly independent vectors not in V. The possibilities of doing this, divided by the number of different ways to choose i linearly independent vectors for the same k-dimensional subspace that contains a fixed $(k-i)$-dimensional subspace, equals

$$\frac{(q^n - q^k)(q^n - q^{k+1}) \dots (q^n - q^{k+i-1})}{(q^k - q^{k-i})(q^k - q^{k-i+1}) \dots (q^k - q^{k-1})},$$

which we can rewrite as

$$\frac{q^k(q^{n-k}-1)q^{k+1}(q^{n-k-1}-1)\dots q^{k+i-1}(q^{n-k-i+1}-1)}{q^{k-i}(q^i-1)q^{k-i+1}(q^{i-1}-1)\dots q^{k-1}(q-1)} = \left(q^i\right)^i \begin{bmatrix} n-k \\ i \end{bmatrix} = q^{i^2} \begin{bmatrix} n-k \\ i \end{bmatrix}.$$

So the cardinality of a shell of the subspaces at distance $2i$ around V is $\begin{bmatrix} k \\ i \end{bmatrix} q^{i^2} \begin{bmatrix} n-k \\ i \end{bmatrix}$. Summing the cardinality of the shells proves the theorem. □

The expression enables us to see immediately that $|\mathcal{S}(n,k,t)| = |\mathcal{S}(n,n-k,t)|$, as expected from (2.2.4).

The next theorem gives the q-analogue of the sphere-packing bound of constant-weight codes.

Theorem 3.1.3 (Sphere-packing bound)**.** *Any (n,M,d,k)-code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ with $d = 2\delta$ and $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$, must satisfy*

$$M \left(\sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix} \right) \leqslant \begin{bmatrix} n \\ k \end{bmatrix},$$

or equivalently

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{S}(n,k,t)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}}.$$

Proof. Let U be an element of $\mathcal{G}_q(n,k)$ in two different spheres $\mathcal{S}(V,k,t)$ and $\mathcal{S}(W,k,t)$ with $V,W \in \mathcal{C}$. Because of the triangle inequality, $d(V,W) \leqslant d(V,U) + d(U,W) \leqslant 4t < 2\delta = d$ and we get a contradiction. So M spheres $\mathcal{S}(V,k,t)$ are mutually disjoint. So

$$|\bigcup_{V\in\mathcal{C}} \mathcal{S}(V,k,t)| = M\left(\sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}\right).$$

This union contains at most $|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}$ subspaces. This proves this theorem. □

We can adapt Definition 1.1.34 for codes in $\mathcal{G}_q(n,k)$.

Definition 3.1.4. A constant-dimension code which achieves the sphere-packing bound is called a ***perfect code***.

Equivalently, we can say that an $(n, M, 2\delta, k)$-code $\mathcal{C}$ is a perfect code if every element of $\mathcal{G}_q(n,k)$ is contained in one and only one sphere $\mathcal{S}(V,k,t)$ with $V \in \mathcal{C}$ and $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$. If we want to emphasize the radius of the sphere, we use the definion of ***t-perfect codes***.

Remark 3.1.5. From the definition it follows that the code which consists of all the k-dimensional spaces in $\mathcal{G}_q(n,k)$ is perfect. So the whole space is always a perfect code. Another trivial perfect code is a single element of $\mathcal{G}_q(n,k)$.

From [7] and [31], respectively [17], we know that for any q, n and k, there are no nontrivial perfect codes in $\mathcal{G}_q(n,k)$ and $\mathcal{P}_q(n)$. We will discuss this in Section 3.3.

Theorem 3.1.6 (Sphere-Covering bound)**.** *There exists an (n, M, d, k)-code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ with $d = 2\delta$ that satisfies*

$$M\left(\sum_{i=0}^{\delta-1} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}\right) \geqslant \begin{bmatrix} n \\ k \end{bmatrix},$$

or equivalently

$$\mathcal{A}_q(n, 2\delta, k) \geqslant \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{S}(n,k,\delta-1)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\sum_{i=0}^{\delta-1} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}}.$$

Proof. Let $\mathcal{C}$ be an optimal (n, M, d, k)-code over a finite field $\mathbb{F}_q$, so $M = \mathcal{A}_q(n, 2\delta, k)$. Since $\mathcal{C}$ has the maximal size, there cannot be a subspace of $\mathcal{G}_q(n,k)$ whose distance from every codeword in $\mathcal{C}$ is at least 2δ. If there was such a subspace, we could include it as a codeword in $\mathcal{C}$ but this contradicts the maximality of the size of $\mathcal{C}$.

Therefore, for every subspace $U \in \mathcal{G}_q(n,k)$ there is at least one codeword $V \in \mathcal{C}$ such that $d(U,V) \leqslant 2\delta - 2$, since the distances between subspaces in $\mathcal{G}_q(n,k)$ are even. Hence, every word in $\mathcal{G}_q(n,k)$ is covered by at least one of the spheres of radius $\delta - 1$ around the codewords $\mathcal{C}$. In other words

$$\mathcal{G}_q(n,k) \subseteq \cup_{V\in\mathcal{C}} \mathcal{S}(V,k,\delta-1).$$

Hence we have

$$\begin{bmatrix} n \\ k \end{bmatrix} \leqslant M \cdot |\mathcal{S}(n,k,\delta-1)|,$$

and the sphere-covering bound follows from Lemma 3.1.2. □

3.1.2 Singleton bound

To prove the Singleton bound in $\mathcal{G}_q(n,k)$ we use the same technique as in the original case, namely, puncturing. So we begin by defining a suitable puncturing operation on constant-dimension codes.

Suppose $\mathcal{C}$ is a subset of $\mathcal{P}_q(n)$, the set of subspaces of a fixed ambient vector space $\mathcal{W}$ of dimension n. Let W' be any subspace of $\mathcal{W}$ of dimension $n-1$. A ***punctured code*** $\mathcal{C}'$ is obtained from $\mathcal{C}$ by replacing each space $V \in \mathcal{C}$ by $V' = \mathcal{H}_{k-1}(V \cap W')$, where $\mathcal{H}_{k-1}$ denotes the erasure operator defined in Definition 2.1.2. This means that V is replaced by $V \cap W'$ if $V \cap W'$ has dimension $k-1$. If $V \subseteq W'$, V is replaced by some $(k-1)$-dimensional subspace of V. Although this puncturing operation does not in general result in a unique code, we denote any such punctured code by $\mathcal{C}|_{W'}$.

Theorem 3.1.7. *If $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ is an (n,M,d,k)-code with $d > 2$ and W' an $(n-1)$-dimensional subspace of $\mathcal{W}$, then $\mathcal{C}' = \mathcal{C}|_{W'}$ is an $(n-1,M,d',k-1)$-code with $d' \geqslant d-2$.*

Proof. It is clear that we only need to verify the cardinality M and the minimum distance d' of $\mathcal{C}'$.

We first prove that $d' \geqslant d-2$. Suppose that U and V are two codewords of $\mathcal{C}$ with corresponding codewords $U' = \mathcal{H}_{k-1}(U \cap W')$ and $V' = \mathcal{H}_{k-1}(V \cap W')$ of $\mathcal{C}'$. Since $U' \subseteq U$ and $V' \subseteq V$, we have $U' \cap V' \subseteq U \cap V$. Together with the property that $d(U,V) = 2k - 2\dim(U \cap V) \geqslant d$, we get

$$2\dim(U' \cap V') \leqslant 2\dim(U \cap V) \leqslant 2k - d.$$

So in $\mathcal{C}'$ we have

$$\begin{aligned} d(U',V') &= \dim(U') + \dim(V') - 2\dim(U' \cap V') \\ &= 2(k-1) - 2\dim(U' \cap V') \\ &\geqslant 2k - 2 - (2k-d) \\ &= d-2. \end{aligned}$$

Since $d > 2$, $d(U',V') > 0$, so U' and V' are distinct, which shows that $\mathcal{C}'$ has indeed as many codewords as $\mathcal{C}$. □

In the next theorem, we give the counterpart of the classical Singleton bound. So from Theorem 3.1.10 it will follow that for all integers $q \geqslant 2$, $n, d = 2\delta$, with $1 \leqslant d \leqslant n$,

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \begin{bmatrix} n-\delta+1 \\ k-\delta+1 \end{bmatrix}. \tag{3.1.1}$$

Most articles use (3.1.1) when they refer to the Singleton bound. With the following lemma, we can describe the Singleton bound in a more precise way, as stated in [28].

Lemma 3.1.8. *For any $n,k,l \in \mathbb{N}$ with $n \geqslant k \geqslant l > 0$ and $n \geqslant k+l$,*

$$\begin{bmatrix} n-l \\ n-k \end{bmatrix} < \begin{bmatrix} n-l \\ k \end{bmatrix} \text{ if and only if } k < n-k.$$

Proof. From Definition 1.4.3 we know that

$$\begin{bmatrix} n-l \\ n-k \end{bmatrix} = \frac{(q^{n-l}-1)(q^{n-l-1}-1)\dots(q^{n-l-(n-k-1)}-1)}{(q^{n-k}-1)(q^{n-k-1}-1)\dots(q-1)}, \tag{3.1.2}$$

$$\begin{bmatrix} n-l \\ k \end{bmatrix} = \frac{(q^{n-l}-1)(q^{n-l-1}-1)\dots(q^{n-l-(k-1)}-1)}{(q^{k}-1)(q^{k-1}-1)\dots(q-1)}. \tag{3.1.3}$$

As we can see (3.1.2) has $n-k$ factors in the numerator and also $n-k$ factors in the denominator and (3.1.3) has k factors in both numerator and denominator.

Suppose $k < n-k$. Then we can rewrite (3.1.2) as

$$\underbrace{\frac{q^{n-l}-1}{q-1}\cdot\frac{(q^{n-l-1}-1)}{q^2-1}\cdots\frac{q^{n-l-(k-1)}-1}{q^k-1}}_{=\begin{bmatrix} n-l \\ k \end{bmatrix}}\cdot\underbrace{\frac{q^{n-l-k}-1}{q^{n-k}-1}\cdot\frac{q^{n-l-k-1}-1}{q^{n-k-1}-1}\cdots\frac{q^{n-l-(n-k-1)}-1}{q^{k+1}-1}}_{<1}.$$

The first k factors give $\begin{bmatrix} n-l \\ k \end{bmatrix}$. The other factors are each less than 1, because the power of q in the numerator is always l less than the power of q in the denominator. So in this case we get

$$\begin{bmatrix} n-l \\ n-k \end{bmatrix} < \begin{bmatrix} n-l \\ k \end{bmatrix}.$$

If $k > n-k$, we just get the other way around. So this proves the lemma. □

Remark 3.1.9. The conditions of Lemma 3.1.8 are only necessary for the existence of the Gaussian coefficients.

Theorem 3.1.10 (Singleton bound)**.** *Any q-ary (n, M, d, k)-code $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, with $d = 2\delta$, must satisfy*

$$|\mathcal{C}| \leqslant \begin{bmatrix} n-\delta+1 \\ \max(k, n-k) \end{bmatrix}.$$

Proof. If $\mathcal{C}$ is punctured $\frac{d-2}{2} = \delta-1$ times, by applying Theorem 3.1.7 exactly $\delta-1$ times, we obtain an $(n-\delta+1, M, d', k-\delta+1)$-code $\mathcal{C}'$, with $d' \geqslant 2$. Since this code cannot have more $(k-\delta+1)$-dimensional codewords than the corresponding Grassmannian $\mathcal{G}_q(n-\delta+1, k-\delta+1)$, it follows that

$$|\mathcal{C}| = |\mathcal{C}'| \leqslant \begin{bmatrix} n-\delta+1 \\ k-\delta+1 \end{bmatrix} = \begin{bmatrix} n-\delta+1 \\ n-k \end{bmatrix}.$$

Applying the same technique to the complementary code $\mathcal{C}^\perp$, the upper bound is $\begin{bmatrix} n-\delta+1 \\ k \end{bmatrix}$. We now verify the conditions of Lemma 3.1.8 for $l = \delta-1$, i.e. $k \geqslant \delta-1$ and $n \geqslant k+\delta-1$. The first condition holds because of the definition of the metric. For the second condition, consider two codewords $U, V \in \mathcal{G}_q(n,k)$ with $d(U,V) = 2\delta$. Since

$$2\delta = d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V) = 2k - 2\dim(U \cap V),$$

it follows that $\dim(U \cap V) = k - \delta$ and so

$$n \geqslant \dim(U+V) = 2k - (k-\delta) = k + \delta \geqslant k + \delta - 1.$$

Then, from Lemma 3.1.8, it follows that $\begin{bmatrix} n-\delta+1 \\ n-k \end{bmatrix} < \begin{bmatrix} n-\delta+1 \\ k \end{bmatrix}$ if and only if $k < n-k$. This implies the Singleton bound. □

3.1.3 Some other bounds

In this subsection, we will improve the sphere-packing bound and the Singleton bound using three completely different methods, but they will all lead to the same result. For this bounds, we rely on the article of Etzion and Vardy [17].

First of all, we consider a more general structure than a sphere in the case of $\mathcal{G}_q(n,k)$.

Definition 3.1.11. An ***anticode*** $\mathscr{A}$ ***of diameter*** r in $\mathcal{G}_q(n,k)$ is any subset of $\mathcal{G}_q(n,k)$ such that $d(U,V) \leqslant 2r$ for all $U,V \in \mathscr{A}$.

Example 3.1.12. An example of such an anticode of diameter r is the sphere $\mathcal{S}(W,k,t)$ for some $W \in \mathcal{G}_q(n,k)$ with $t = \frac{r}{2}$. This follows from the triangle inequality, since for all $U,V \in \mathcal{S}(W,k,t)$, necessarily

$$d(U,V) \leqslant d(U,W) + d(W,V) \leqslant 2t + 2t = 2r.$$

As the sphere is an example of an anticode, the sphere-packing bound is a special case of the anticode bound. This bound was shown by Delsarte for arbitrary association schemes in [13]. In this work, he proved the following result.

Theorem 3.1.13 (Delsarte)**.** *Let X and Y be subsets of the vertex set V of a distance regular graph Γ, such that the nonzero distances occurring between vertices of X do not occur between vertices of Y. Then*

$$|X||Y| \leqslant |V|.$$

In particular, this theorem implies the next corollary, when we set X as a code $\mathcal{C}$ with minimum distance 2δ and Y an anticode $\mathscr{A}$ of diameter $\delta - 1$.

Corollary 3.1.14.

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \frac{|\mathcal{G}_q(n,k)|}{|\mathscr{A}(\delta-1)|}$$

for any anticode $\mathscr{A}(\delta-1)$ of diameter $\delta - 1$.

If we take the sphere $\mathcal{S}(W,k,t)$ as anticode in the previous inequality, with $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$, we get indeed the sphere-packing bound.

In the binary Hamming space, spheres are the largest anticodes[1]. But that is not true in $\mathcal{G}_q(n,k)$, on the contrary, these spheres $\mathcal{S}(n,k,t)$ are small anticodes in $\mathcal{G}_q(n,k)$. To find the largest anticode in $\mathcal{G}_q(n,k)$, we will make use of the results of the q-analogues of Erdős-Ko-Rado sets (see Section 1.4). Combining this with Corollary 3.1.14 gives us an improvement of the sphere-packing bound. In [42], they proved that this bound is even stronger than the Singleton bound.

[1] In the case of the Hamming space, the anticode A of diameter r will be defined as the subset of $\mathbb{F}_q^n$ such that $d(x,y) \leqslant 2r$ for all $x,y \in A$.

Theorem 3.1.15.

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

Proof. An anticode of diameter $\delta - 1$ is a set of k-dimensional subspaces such that for every $U, V \in \mathcal{G}_q(n, k)$,

$$d(U, V) = 2k - 2\dim(U \cap V) \leqslant 2(\delta - 1),$$

or equivalently,

$$\dim(U \cap V) \geqslant k - \delta + 1.$$

Theorem 1.4.5 shows that the largest anticode of diameter $\delta-1$ is the set of all subspaces with dimension k, containing a fixed $(k-\delta+1)$-dimensional subspace of $V(n, q)$, with size $\begin{bmatrix} n-k+\delta-1 \\ \delta-1 \end{bmatrix}$. Applying Corollary 3.1.14 for this anticode and we get the theorem. □

Another way of improving the sphere-packing bound is the next theorem, which is based upon a standard covering argument.

Theorem 3.1.16.

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}}. \tag{3.1.4}$$

Proof. Let $\mathcal{C}$ be an $(n, M, 2\delta, k)$-code. Each codeword of $\mathcal{C}$ contains exactly $\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}$ subspaces of dimension $k - \delta + 1$. But a given $(k - \delta + 1)$-dimensional subspace of $\mathbb{F}_q^n$ cannot be contained in two distinct elements $U, V \in \mathcal{C}$, since otherwise

$$d(U, V) = 2k - 2\dim(U \cap V) \leqslant 2k - 2(k - \delta + 1) = 2\delta - 2.$$

The total number of subspaces of $\mathbb{F}_q^n$ of dimension $k-\delta+1$ is $\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}$. This implies that M cannot be larger than $\frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}}$. □

Remark 3.1.17. It is clear from the proof of the above theorem that if $\mathcal{C}$ attains the bound of (3.1.4), then every subspace of $\mathbb{F}_q^n$ of dimension $k-\delta+1$ must be contained in exactly one codeword of $\mathcal{C}$. Such codes are called Steiner structures. We discuss this in Chapter 4 and 5.

The third theorem of this section gives again a better bound for the maximum number of codewords in an (n, M, d, k)-code in $\mathcal{G}_q(n, k)$. It uses iteratively Theorem 3.1.19, which is shown in the next subsection.

Theorem 3.1.18.

$$\mathcal{A}_q(n, 2\delta, k) \leqslant \prod_{i=0}^{k-\delta} \frac{q^{n-i} - 1}{q^{k-i} - 1}.$$

Proof. Apply Theorem 3.1.19 iteratively $k-\delta+1$ times, stopping with the trivial equality $\mathcal{A}_q(n-k+\delta-1, 2\delta, \delta-1) = 1$, since for two different codewords U and V of an $(n-k+\delta-1, M, 2\delta, \delta-1)$-code $\mathcal{C}$ it would follow that

$$d(U,V) = 2(\delta-1) - 2\dim(U \cap V) \leqslant 2\delta - 2. \qquad \square$$

We have discussed these three bounds together in this subsection, because we can verify directly from the definition of the Gaussian coefficient that

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\begin{bmatrix} n-k+\delta-1 \\ \delta-1 \end{bmatrix}} = \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}} = \prod_{i=0}^{k-\delta} \frac{q^{n-i}-1}{q^{k-i}-1},$$

so the three theorems give the same result. These bounds are always stronger than the Singleton bound and the sphere-packing bound ([42]).

Furthermore, in the next section we shall see that we can still improve these bounds a little bit.

3.1.4 Johnson bounds

The three following theorems are the q-analogues in $\mathcal{G}_q(n,k)$ of the classical Johnson bounds for constant-weight codes (see Subsubsection 1.1.3.3).

Theorem 3.1.19.

$$\mathcal{A}_q(n,d,k) \leqslant \frac{q^n-1}{q^k-1}\mathcal{A}_q(n-1,d,k-1).$$

Proof. Let $\mathcal{C}$ be an (n,M,d,k)-code in $\mathcal{G}_q(n,k)$, and suppose that $M = \mathcal{A}_q(n,d,k)$. The number of one-dimensional subspaces of $\mathbb{F}_q^n$ which are contained in each (k-dimensional) codeword of $\mathcal{C}$ is $\frac{q^k-1}{q-1}$. Since the total number of such subspaces is $\frac{q^n-1}{q-1}$, the mean of codewords in which a one-dimensional subspace is contained is

$$M \cdot \frac{q^k-1}{q-1} \cdot \frac{q-1}{q^n-1}.$$

So there is a one-dimensional subspace $\mathcal{X} \in \mathcal{G}_q(n,1)$ that is contained in at least $M \cdot \frac{q^k-1}{q^n-1}$ codewords of $\mathcal{C}$. Assume that $\mathcal{X}$ is spanned by a vector $x \in \mathbb{F}_q^n$, so $\mathcal{X} = \langle x \rangle$. We can write $\mathbb{F}_q^n = \mathcal{X} \oplus \mathcal{Y}$ for some $\mathcal{Y} \in \mathcal{G}_q(n,n-1)$, because we can take for example the basis $\{x, e_1, \ldots, e_{n-1}\}$ for $\mathbb{F}_q^n$ and set $\mathcal{Y} = \langle e_1, e_2, \ldots, e_{n-1} \rangle$. Let us now define

$$\mathcal{C}' \coloneqq \{V \cap \mathcal{Y} | V \in \mathcal{C} \text{ and } \mathcal{X} \subset V\}.$$

From this definition all codewords of $\mathcal{C}$ are contained in $\mathcal{Y}$ and since $\mathcal{X} \nsubseteq \mathcal{Y}$, every codeword in $\mathcal{C}'$ is $k-1$-dimensional. So C' can be seen as an $(n-1, M', d', k-1)$-code, where $M' \geqslant M\frac{q^k-1}{q^n-1}$ by our choice of $\mathcal{X}$. If we can show that $d' = d$, it would follow that

$$\mathcal{A}_q(n,d,k) \leqslant \frac{q^n-1}{q^k-1}\mathcal{A}_q(n-1,d,k-1).$$

In fact, it is sufficient to show that $d' \geqslant d$. Indeed, if C' would be an $(n-1, M', d', k-1)$-code with $d' > d$, take two spaces at the minimum distance d' and change one of them in such a way that the distance between the two spaces decrease to d.

Now, in order to proof that $d' \geqslant d$, we consider two arbitrary codewords $U', V' \in \mathcal{C}'$ such that $U' = U \cap \mathcal{Y}$ and $V' = V \cap \mathcal{Y}$, with corresponding codewords in $\mathcal{C}$ such that $\mathcal{X} \subset U$ and $\mathcal{X} \subset V$. Note that $U' \cap V' = (U \cap \mathcal{Y}) \cap (V \cap \mathcal{Y}) = (U \cap V) \cap \mathcal{Y}$, so we get

$$\dim(U' \cap V') = \dim(U \cap V) + \dim(\mathcal{Y}) - \dim((U \cap V) + \mathcal{Y}).$$

Since $\mathcal{X}$ is contained in $U \cap V$, $\mathbb{F}_q^n = (U \cap V) + \mathcal{Y}$ and it follows that

$$\dim(U' \cap V') = \dim(U \cap V) + (n-1) - n = \dim(U \cap V) - 1.$$

This implies that

$$\begin{aligned} d(U', V') &= \dim(U') + \dim(V') - 2\dim(U' \cap V') \\ &= k - 1 + k - 1 - 2(\dim(U \cap V) - 1) \\ &= 2k - 2\dim(U \cap V) \\ &= d(U, V) \\ &\geqslant d, \end{aligned}$$

so $d' \geqslant d$. □

The next bound will be proved in two different ways. The first uses techniques akin to the proof of Theorem 3.1.19. The proof of the second counterpart of the Johnson bound can be proved easier by using Theorem 3.1.19, as you will see in the second proof of the following theorem. Remark that this technique is similar to the proof of Theorem 1.1.40, which also uses complementary codes.

Theorem 3.1.20.

$$\mathcal{A}_q(n, d, k) \leqslant \frac{q^n - 1}{q^{n-k} - 1} \mathcal{A}_q(n-1, d, k).$$

Proof 1. Assume that $\mathcal{C}$ is an (n, M, d, k)-code with $M = \mathcal{A}_q(n, d, k)$. Take an arbitrary $\mathcal{Y} \in \mathcal{G}_q(n, n-1)$ and define the code

$$\mathcal{C}_{\mathcal{Y}} \coloneqq \{V | V \in \mathcal{C} \text{ and } V \subset \mathcal{Y}\}.$$

For each $\mathcal{Y} \in \mathcal{G}_q(n, n-1)$, this code $\mathcal{C}_{\mathcal{Y}}$ is an $(n-1, M_{\mathcal{Y}}, d', k)$-code with $d' \geqslant d$. Any given k-dimensional subspace U of $\mathbb{F}_q^n$ is contained in precisely $\frac{q^{n-k}-1}{q-1}$ elements of $\mathcal{G}_q(n, n-1)$. Since

$$\frac{(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{n-2})}{(q^{n-1} - q^k)(q^{n-1} - q^{k+1}) \cdots (q^{n-1} - q^{n-2})} = \frac{q^k q^{k+1} \dots q^{n-2}(q^{n-k} - 1) \cdots (q^2 - 1)}{q^k q^{k+1} \dots q^{n-2}(q^{n-k-1} - 1) \cdots (q - 1)}$$

is the number of possibilities to choose $n-1-k$ vectors that extend U to an $(n-1)$-dimensional subspace, divided by the number of possibilities to choose $n-1-k$ vectors

that extend U to the same $(n-1)$-dimensional subspace. Thus, each codeword of $\mathcal{C}$ is also a codeword of $\frac{q^{n-k}-1}{q-1}$ different codes $\mathcal{C}_\mathcal{Y}$. Therefore, we get

$$\sum_{\mathcal{Y}} |\mathcal{C}_\mathcal{Y}| = M\frac{q^{n-k}-1}{q-1},$$

where the sum is taken over all the $\frac{q^n-1}{q-1}$ elements of $\mathcal{G}_q(n,n-1)$. Hence, there exists at least one $\mathcal{Y} \in \mathcal{G}_q(n,n-1)$ such that

$$|\mathcal{C}_\mathcal{Y}| \geqslant M\frac{q^{n-k}-1}{q^n-1}.$$

The theorem follows from the fact that, for all $\mathcal{W} \in \mathcal{G}_q(n,n-1)$,

$$\mathcal{A}_q(n-1,d,k) \geqslant |\mathcal{C}_\mathcal{Y}| \geqslant \mathcal{A}_q(n,d,k)\frac{q^{n-k}-1}{q^n-1}.$$ □

The next proof of Theorem 3.1.20 uses the first counterpart of the classical Johnson bound, Theorem 3.1.19, and the observation that $d(U^\perp,V^\perp) = d(U,V)$, as shown in (2.2.4).

Proof 2. If $\mathcal{C}$ is an (n,M,d)-code in $\mathcal{P}_q(n)$, then its orthogonal complement $\mathcal{C}^\perp$ is also an (n,M,d)-code, as observed in Subsection 2.2.2, so $\mathcal{A}_q(n,2\delta,k) = \mathcal{A}_q(n,2\delta,n-k)$. It follows from Theorem 3.1.19 that

$$\mathcal{A}_q(n,d,n-k) \leqslant \frac{q^n-1}{q^{n-k}-1}\mathcal{A}_q(n-1,d,n-k-1).$$

But again, since the size of a code is the same as the size of its complementary code, we have $\mathcal{A}_q(n-1,2\delta,n-k-1) = \mathcal{A}_q(n-1,2\delta,k)$. This leads us to 3.1.20. □

If we iterate Theorem 3.1.19 and Theorem 3.1.20, we obtain a bound on $\mathcal{A}_q(n,2\delta,k)$ for any n,k and d. But it is still an open problem to find in which order they should be iterated to get the best bound, even for the problem in the Johnson space. However, we can just iterate Theorem 3.1.19 with itself. Combining this with the observation that for all $k < \delta$ we have $\mathcal{A}_q(n,2\delta,k) = 1$, this gives us the following bound. Note that the limit $q \to 1$ will give us Corollary 1.1.39.

Theorem 3.1.21.

$$\mathcal{A}_q(n,2\delta,k) \leqslant \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+\delta}-1}{q^\delta-1} \right\rfloor \cdots \right\rfloor \right\rfloor.$$

Remark 3.1.22. Note that if we ignore all the floors in Theorem 3.1.21, we simply get Theorem 3.1.18. This means that Theorem 3.1.21 is always at least as strong, and usually stronger, as the theorems in Subsection 3.1.3.

3.2 Bounds on codes in projective space

In the previous section we gave analogons in $\mathcal{G}_q(n,k)$ for classical bounds of coding theory. It is not trivial to generalize this to bounds in $\mathcal{P}_q(n)$, since we already noticed in Remark 2.2.9 that spheres of the same radius in $\mathcal{P}_q(n)$ can have different sizes. That is the reason why we cannot use the same technique for the q-analogue of the sphere-packing bound in $\mathcal{P}_q(n)$ as in Theorem 3.1.3. Also for other bounds, the q-analogue is still an open problem. However, for the sphere-covering bound, Etzion and Vardy get around the problems of different sizes of spheres by using the 'average size of a sphere', which is done in [17].

Working towards Theorem 3.2.5, we will start by giving the definition of a sphere in $\mathcal{P}_q(n)$.

Definition 3.2.1. Let $V \in \mathcal{P}_q(n)$ be a subspace of the ambient n-dimensional vector space $\mathcal{W}$. The ***sphere*** $\boldsymbol{\mathcal{S}_r(V)}$ of radius r centered at $V \in \mathcal{P}_q(n)$ is defined as

$$\mathcal{S}_r(V) \coloneqq \{U \in \mathcal{P}_q(n) | d(U,V) \leqslant r\}. \tag{3.2.1}$$

As we did in the case of constant-dimension codes, we want to determine the size of this sphere $\mathcal{S}_r(V)$.

Let $\boldsymbol{c(j,k,r)}$ denote the number of j-dimensional subspaces in a sphere of radius r around a k-dimensional subspace of $\mathbb{F}_q^n$. That is, $c(j,k,r) = |\mathcal{S}_r(V) \cap \mathcal{G}_q(n,j)|$ for all $V \in \mathcal{G}_q(n,k)$. Note that the number of elements in $\mathcal{S}(n,k,t)$ is $c(k,k,2t)$.

Lemma 3.2.2.

$$c(j,k,r) = \sum_{i=\lceil \frac{k+j-r}{2} \rceil}^{\min(j,k)} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}.$$

Proof. For a given $V \in \mathcal{G}_q(n,k)$, the number of ways to choose an i-dimensional subspace U of V, with $i \leqslant k$, is $\begin{bmatrix} k \\ i \end{bmatrix}$. Fix such a U and assume $i \leqslant j$. The number of subspaces $U' \in \mathcal{G}_q(n,j)$ such that $V \cap U' = U$ is the number of ways to extend U to some U', i.e. the number of $(j-i)$-tuples of linearly independent vectors not in V, divided by the number of possibilities to choose these vectors to achieve the same U', i.e. the number of ways to choose $j-i$ linearly independent vectors in a j-dimensional subspace U' not in a subspace U of dimension i. This is

$$\frac{(q^n-q^k)(q^n-q^{k+1})\cdots(q^n-q^{k+j-i-1})}{(q^j-q^i)(q^j-q^{i+1})\cdots(q^j-q^{j-1})} = \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}. \tag{3.2.2}$$

One achieves the equation by taking q^k out of a factor in the numerator and q^i out of a factor in the denominator and doing this $j-i$ times. Since the vector spaces V and U' have to be in a sphere of radius r,

$$d(V,U') = \dim(V) + \dim(U') - 2\dim(V \cap U') = k + j - 2i \leqslant r$$

and this only holds if and only if $i \geqslant \frac{k+j-r}{2}$. Note that at the beginning of this proof, we assumed $i \leqslant j$ and $i \leqslant k$, so $i \leqslant \min(j,k)$. Hence summing over i brings us to the lemma.

□

Lemma 3.2.3. *For all $V \in \mathcal{P}_q(n)$ with $\dim V = k$, we have*

$$|\mathcal{S}_r(V)| = \mathcal{S}_{k,r} := \sum_{j=0}^{r} \sum_{i=0}^{j} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)},$$

in which we set $\begin{bmatrix} k \\ i \end{bmatrix} = 0$, by convention, for $i \notin \{0, 1, \ldots, k\}$.

Proof. We obtain $|\mathcal{S}_r(V)|$ by taking the sum over all $c(j,k,r)$ for $j = 0, \ldots, n$. From Lemma 3.2.2, it follows that

$$|\mathcal{S}_r(V)| = \sum_{j=0}^{n} c(j,k,r) = \sum_{(i,j)\in S} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}, \tag{3.2.3}$$

with

$$S = \{(i,j) \in \mathbb{Z}^2 | 0 \leqslant j \leqslant n \text{ and } \left\lceil \frac{k+j-r}{2} \right\rceil \leqslant i \leqslant \min(j,k)\}.$$

Taking the sum over a set

$$S' = \{(i,j) \in \mathbb{Z}^2 | 0 \leqslant j \leqslant n \text{ and } \max(0, \left\lceil \frac{k+j-r}{2} \right\rceil) \leqslant i \leqslant \min(j,k)\}$$

does not change (3.2.3), because $\begin{bmatrix} k \\ i \end{bmatrix} = 0$ for $i < 0$. Note that if $j < 0$, it follows that $j - i < -i \leqslant 0$ and $\begin{bmatrix} n-k \\ j-i \end{bmatrix} = 0$, and if $j > n$, it follows that $j - i > n - i \geqslant n - k$ and then also $\begin{bmatrix} n-k \\ j-i \end{bmatrix} = 0$. These observations give us the opportunity to set no restrictions on j in the adapted subset of $\mathbb{Z}^2$, over which we take the sum. The only remaining condition for $(i,j) \in \mathbb{Z}^2$ is the lower bound $\lceil \frac{k+j-r}{2} \rceil$ for i, because if $i < 0$ or $i > k$, $\begin{bmatrix} k \\ i \end{bmatrix} = 0$ and if $i > j$, then $\begin{bmatrix} n-k \\ j-i \end{bmatrix} = 0$ since $j - i < 0$.

This means that $|\mathcal{S}_r(V)| = \sum_{(i,j)\in S''} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}$, with a set S'' equal to

$$\{(i,j) \in \mathbb{Z}^2 | i \geqslant \left\lceil \frac{k+j-r}{2} \right\rceil\} = \{(i,j) \in \mathbb{Z}^2 | 2i \geqslant k+j-r\} = \{(i,j) \in \mathbb{Z}^2 | k+j-2i \leqslant r\}.$$

By substituting $j' := j + k - 2i$, we get

$$|\mathcal{S}_r(V)| = \sum_{i\in\mathbb{Z}} \sum_{j'\leqslant r} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j'-k+i \end{bmatrix} q^{(j'-k+i)(k-i)}.$$

Another substitution $i' := k - i$ leads us to

$$\sum_{i'\in\mathbb{Z}} \sum_{j'\leqslant r} \begin{bmatrix} k \\ k-i' \end{bmatrix} \begin{bmatrix} n-k \\ j'-i' \end{bmatrix} q^{(j'-i')i'} = \sum_{j'\leqslant r} \sum_{i'\in\mathbb{Z}} \begin{bmatrix} k \\ k-i' \end{bmatrix} \begin{bmatrix} n-k \\ j'-i' \end{bmatrix} q^{(j'-i')i'}.$$

Recall the property of the Gaussian coefficient, $\begin{bmatrix} k \\ k-i' \end{bmatrix} = \begin{bmatrix} k \\ i' \end{bmatrix}$, and the fact that $\begin{bmatrix} k \\ i' \end{bmatrix} = 0$ if $i' < 0$ and $\begin{bmatrix} n-k \\ j'-i' \end{bmatrix} = 0$ if $j' - i' < 0$. This proves the lemma. □

To prove the counterpart of sphere-covering bound[2], we use the work of Tolhuizen ([36]), which extends the Gilbert-Varshamov bound to graphs that are not necessarily distance-regular. In [36], Tolhuizen establishes the following intuitive, but not obvious, result.

Theorem 3.2.4. *If $\overline{\mathcal{S}}_r$ is the* **average size** *of a sphere of radius r in a graph $G = (V, E)$, then there exists a code $\mathcal{C}$ in G with minimum (graph) distance d and*

$$|\mathcal{C}| \geqslant \frac{|V|}{\overline{\mathcal{S}}_{d-1}}.$$

This implies the following theorem.

Theorem 3.2.5.

$$\mathcal{A}_q(n,d) \geqslant \frac{\sum_{k=0}^{n}\sum_{j=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} n \\ j \end{bmatrix}}{\sum_{k=0}^{n}\sum_{j=0}^{d-1}\sum_{i=0}^{j}\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} k \\ i \end{bmatrix}\begin{bmatrix} n-k \\ j-i \end{bmatrix}q^{i(j-i)}}.$$

Proof. Note that $\mathcal{P}_q(n) = \cup_{k=0}^{n}\mathcal{G}_q(n,k)$ and so $|\mathcal{P}_q(n)| = \sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}$. In the case of $\mathcal{P}_q(n)$, in the relevant graph $G = (V, E)$,

$$|V| = |\mathcal{P}_q(n)| = \sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}$$

and the average size of a sphere of radius $d-1$ in G is

$$\begin{aligned}\overline{\mathcal{S}}_{d-1} &= \frac{\sum_{V\in\mathcal{P}_q(n)}|\mathcal{S}_{d-1}(V)|}{|\mathcal{P}_q(n)|} = \frac{1}{|\mathcal{P}_q(n)|}\sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}\mathcal{S}_{k,d-1} \\ &= \frac{\sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}\sum_{j=0}^{d-1}\sum_{i=0}^{j}\begin{bmatrix} k \\ i \end{bmatrix}\begin{bmatrix} n-k \\ j-i \end{bmatrix}q^{i(j-i)}}{\sum_{j=0}^{n}\begin{bmatrix} n \\ j \end{bmatrix}}.\end{aligned}$$

We use Theorem 3.2.4 and we obtain immediately the derived inequality. □

3.3 Perfect codes

In Subsection 3.1.1 we already mentioned the concept of perfect codes for constant-dimension codes. These codes achieve, by definition, the sphere-packing bound. This means that an $(n, M, 2\delta, k)$-code $\mathcal{C}$ is a perfect code if and only if every element of $\mathcal{G}_q(n,k)$ is contained in one and only one sphere $\mathcal{S}(V,k,t)$ with $V \in \mathcal{C}$ and $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$.

To generalize the definition for all codes in projective space, we use the concept of the sphere as in Definition 3.2.1.

[2]The sphere-covering bound is often denoted as (the weaker version of) the Gilbert-Varshamov bound.

Definition 3.3.1. An (n, M, d)-code $\mathcal{C}$ of $\mathcal{P}_q(n)$ is said to be e-perfect if the spheres of radius e centered at the codewords both pack and cover $\mathcal{P}_q(n)$, or, in other words, if every element of $\mathcal{P}_q(n)$ is contained in one and only one sphere $\mathcal{S}_e(V), V \in \mathcal{C}$.

For any q or n, there are always two trivial perfect codes in $\mathcal{P}_q(n)$. The whole space is 0-perfect, and any single element of $X \in \mathcal{P}_q(n)$ gives an n-perfect code. When $n = 2e+1$, the binary Hamming space and the Johnson space $\mathcal{J}(2n, n)$ (see Subsection 1.1.3) admit a third type of a trivial perfect code. Also in the case of $\mathcal{P}_q(n)$, we have another example of perfect codes, i.e. the code consisting of the null-space $\{0\}$ and $\mathbb{F}_q^n$. Nevertheless, in the Grassmannians we do not have a third example of such trivial perfect codes.

In the next subsections we discuss the fact that there are no more perfect codes than the trivial ones stated above. The main part of this section about perfect codes is the proof of the nonexistence of nontrivial codes in $\mathcal{P}_q(n)$ of Etzion and Vardy [17]. But first, we give a sketch of the method used in [31] which shows that nontrivial perfect codes in the special case of the Grassmannian do not exist.

3.3.1 Nonexistence of nontrivial perfect codes in $\mathcal{G}_q(n, k)$

In [7] Chihara proved that many infinite families of classical distance-regular graphs do not have nontrivial perfect codes. This includes that the Grassmann graph do not have perfect codes and that, consequently, nontrivial perfect codes do not exist in the Grassmannian. Chihara used a technique with zeroes of Askey-Wilson polynomials.

In [31] the same result for Grassmann graphs (and also for bilinear forms graphs) is proved, but in a different, more elementary way. Martin and Zhu used Delsarte's anticode condition (see Theorem 3.1.13), i.e. if for two nonempty subsets X and Y of the set of vertices of a distance-regular graph $G(V, E)$ and for each distance $i \geqslant 1$, at least one of the two sets contains no pair of vertices at distance i, then

$$|X||Y| \leqslant |V|.$$

To use Delsarte's Theorem, we introduce the concept of an e-perfect code and an anticode of a graph G.

Definition 3.3.2. An ***e-perfect code*** in a graph G is a subset X of the vertices such that every vertex of G is at distance e or less from one and only one element of X.

This definition implies that an e-perfect code contains no pair of vertices at distance i, for $1 \leqslant i \leqslant 2e$, since the minimum distance is equal to $d = 2e+1$. Moreover, an e-perfect code in a distance-regular graph has size $\frac{|V|}{|S_e|}$, where S_e is a sphere of radius e around any vertex, since every element of V has to be in exactly one such sphere S_e.

Definition 3.3.3. In a graph $G(V, E)$, any subset Y of V such that the maximum distance between elements of Y is at most δ is called an ***anticode of diameter δ***.

Remark 3.3.4. Also note that in Definition 3.1.11, an anticode in $\mathcal{G}_q(n, k)$ of radius r consists of a subset of elements of $\mathcal{G}_q(n, k)$ such that the maximum distance between two different elements is at most $2r$. This is not a surprise, since we know that the distance in the Grassmann graph is half of the distance in the Grassmannian $\mathcal{G}_q(n, k)$ (see Definition 2.2.8).

Theorem 3.1.13 can now be used with an anticode of diameter δ and any code of minimum distance at least $\delta + 1$. To study the existence of perfect codes, i.e. to prove that there are no nontrivial perfect codes in the Grassmann graph, we can make use of the theorem of Delsarte. Let X be an e-perfect code. If there exists an anticode of diameter at most $2e$ with a cardinality larger than $|S_e|$, this will be sufficient to prove that the graph has no e-perfect code. Since $|X| = \frac{|V|}{|S_e|}$, then we find a contradiction with Delsarte's theorem. And indeed, in [31], Martin and Zhu give an anticode Y of a Grassmann graph $G_q(n,k)$ of diameter $2e$, having a cardinality such that $|Y| - |S_e|$ is always strictly positive.

3.3.2 Nonexistence of nontrivial perfect codes in $\mathcal{P}_q(n)$

We already noted in Remark 2.2.9 that $\mathcal{P}_q(n)$ is not distance-regular, so the methods based upon association schemes and distance-regular graphs, as in [7] and Subsection 3.3.1, cannot be applied. Therefore, in [17], completely different techniques are used. Based on that article, we explain in this section how Etzion and Vardy did this, starting with the following lemma.

Lemma 3.3.5.

$$\mathcal{A}_q(n, 2k, k) \leqslant \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor - 1 \qquad \text{if } n \not\equiv 0 \pmod{k}.$$

Proof. Write $n = mk + r$, where r is the remainder obtained dividing n by k and by assumption, $0 < r < k$. Now assume to the contrary that there exists an $(n, M, 2k, k)$-code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ with $M = \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor$. Since

$$\begin{aligned}
\frac{q^n - 1}{q^k - 1} &= \frac{q^n - q^{n-k}}{q^k - 1} + \frac{q^{n-k} - 1}{q^k - 1} \\
&= q^{n-k} + \frac{q^{n-k} - q^{n-2k}}{q^k - 1} + \frac{q^{n-2k} - 1}{q^k - 1} \\
&= \cdots \\
&= q^{n-k} + q^{n-2k} + \ldots + q^{n-mk} + \frac{q^r - 1}{q^k - 1},
\end{aligned} \tag{3.3.1}$$

it follows that $M = q^{n-k} + q^{n-2k} + \ldots + q^{n-mk}$. Furthermore, denote by $V_1, V_2, \ldots, V_M$ the codewords of $\mathcal{C}$. Since $d(V_i, V_j) = \dim(V_i) + \dim(V_j) - 2\dim(V_i \cap V_j) \geqslant 2k$ for different codewords $V_i, V_j \in \mathcal{G}_q(n,k)$, it follows that $V_i \cap V_j = \{0\}$ for all $i \neq j$. This implies a partition of $\mathbb{F}_q^n \backslash \{0\}$ into $M + 1$ disjoint sets in the following way. For all i, define $V_i^* = V_i \backslash \{0\}$. These sets V_i^*, together with the set $X \subseteq \mathbb{F}_q^n$ of all vectors in $\mathbb{F}_q^n$ that are not contained in any codeword of $\mathcal{C}$, partition $\mathbb{F}_q^n \backslash \{0\}$, or in other words

$$\mathbb{F}_q^n \backslash \{0\} = V_1^* \cup V_2^* \cup \cdots \cup V_M^* \cup X. \tag{3.3.2}$$

The observations (3.3.2) and (3.3.1) imply the size of X, that is

$$\begin{aligned}|X| &= |\mathbb{F}_q^n \backslash \{0\}| - M \cdot (q^k - 1) \\ &= q^n - 1 - \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor \cdot (q^k - 1) \\ &= (q^{n-k} + q^{n-2k} + \ldots + q^{n-mk}) \cdot (q^k - 1) + q^r - 1 \\ &\quad - (q^{n-k} + q^{n-2k} + \ldots + q^{n-mk}) \cdot (q^k - 1) \\ &= q^r - 1.\end{aligned}$$

Consider a fixed nonzero vector $u \in \mathbb{F}_q^n$ and a set $S \subset \mathbb{F}_q^n$ and denote by $\eta_u(S)$ the number of vectors in S that are not orthogonal to u, i.e.

$$\eta_u(S) \coloneqq |\{x \in S | \langle x, u \rangle \neq 0\}|,$$

where the inner product is over $\mathbb{F}_q$. Note that $\eta_u(V_i^*) = \eta_u(V_i)$, for all i. This value is zero if $V_i \subseteq u^\perp$ or, if not every vector of V_i is in the orthogonal complement of u,

$$\eta_u(V_i) = |V_i| - |V_i \cap u^\perp| = q^k - q^{k-1} = (q-1)q^{k-1}.$$

Furthermore, since every nonzero vector of $\mathbb{F}_q^n$ is never orthogonal with all vectors of $\mathbb{F}_q^n$, $\eta_u(\mathbb{F}_q^n) = (q-1)q^{n-1}$. Therefore

$$\eta_u(X) = \eta_u(\mathbb{F}_q^n \backslash \{0\}) - \sum_{i=1}^{M} \eta_u(V_i^*)$$

is divisible by q^{k-1}. But since $|X| = q^r - 1 < q^k - 1$, this implies that $\eta_u(X) = 0$. This holds for all nonzero $u \in \mathbb{F}_q^n$, from which it follows that the set X cannot contain any nonzero vectors. But this contradicts the fact that $|X| = q^r - 1$ with $0 < r < k$, and so the inequality of the lemma follows. □

Now we are ready to prove that the only perfect codes in a projective space $\mathcal{P}_q(n)$ for given q and n, are the trivial perfect codes.

Theorem 3.3.6. *For all q and n, there are no nontrivial perfect codes in the projective space $\mathcal{P}_q(n)$.*

Proof. Let us assume to the contrary that $\mathcal{C}$ is a nontrivial e-perfect code in $\mathcal{P}_q(n)$. Write $d = 2e + 1$ and define

$$\mathcal{C}_k \coloneqq \mathcal{C} \cap \mathcal{G}_q(n, k), \qquad k = 0, 1, \ldots, n.$$

We distinguish between two cases, i.e. whether $\{0\}$ is an element of the code, or not.

Case 1. $\{0\} \in \mathcal{C}$.

We have $\mathcal{C}_1 = \mathcal{C}_2 = \cdots = \mathcal{C}_{2e} = \emptyset$, because otherwise, there would be two different codewords in the sphere around the codeword $\{0\}$. This means also that for $i \leqslant e$, every i-dimensional subspace is contained in the sphere $\mathcal{S}_e(\{0\})\}$. On the other hand, an $(e+1)$-dimensional subspace U cannot be contained in $\mathcal{S}_e(\{0\})$, since $d(U, \{0\}) = e + 1$.

Furthermore, this subspace U can also not be contained in a sphere $\mathcal{S}_e(V)$, for a codeword V of dimension larger than or equal to $d+1 = 2e+2$. Indeed, otherwise

$$d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V) \geqslant e+1+2e+2-2(e+1) = e+1.$$

Consequently, every element of $\mathcal{G}_q(n, e+1)$ has to be covered by exactly one sphere centered at a codeword of $\mathcal{C}_d$. Moreover, if there is an arbitrary subspace $U \in \mathcal{G}_q(n, e+1)$ in the sphere $\mathcal{S}_e(V)$ for a codeword $V \in \mathcal{C}_d$, such that $\dim(U \cap V) \leqslant e$, then it follows that $d(U,V) \geqslant e+1+2e+1-2e = e+2$, which gives a contradiction. This means that in this case, U has to be contained in such a d-dimensional codeword V. Therefore we can say that every element of $\mathcal{G}_q(n, e+1)$ has to be covered by a codeword of $\mathcal{C}_d$. This structure is called a Steiner structure $\mathscr{S}_q(e+1, d, n)$[3]. Since the number of $(e+1)$-dimensional subspaces in $\mathcal{P}_q(n)$ is $\begin{bmatrix} n \\ e+1 \end{bmatrix}$ and every codeword in $\mathcal{C}_d$ covers exactly $\begin{bmatrix} d \\ e+1 \end{bmatrix}$ such subspaces, we have[4]

$$|\mathcal{C}_d| = \frac{\begin{bmatrix} n \\ e+1 \end{bmatrix}}{\begin{bmatrix} d \\ e+1 \end{bmatrix}} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-e}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q^{d-e}-1)}.$$

For the subspaces U' of $\mathcal{G}_q(n, e+2)$ and a codeword $V' \in \mathcal{G}_q(n, 2e+3)$, it follows that

$$d(U',V') = e+2+(2e+3)-2\dim(U' \cap V') \geqslant e+1,$$

so we find analogously that every $(e+2)$-dimensional subspace has to be contained in a sphere $\mathcal{S}_e(V)$, for a codeword V with $\dim(V) \leqslant 2e+2$. If $U \in \mathcal{G}_q(n, e+2)$, $V \in \mathcal{C}_d$ and $\dim(U \cap V) \leqslant e+1$, then $d(U,V) \geqslant e+2+2e+1-2(e+1) = e+1$. Therefore, every $(e+2)$-dimensional subspace in a sphere with radius e and centered at a d-dimensional codeword, has to be a subspace of that codeword. Each subspace of $\mathcal{C}_d$ covers $\begin{bmatrix} d \\ e+2 \end{bmatrix}$ elements of $\mathcal{G}_q(n, e+2)$. Therefore, there remain $\begin{bmatrix} n \\ e+2 \end{bmatrix} - |\mathcal{C}_d| \cdot \begin{bmatrix} d \\ e+2 \end{bmatrix}$ elements of $\mathcal{G}_q(n, e+2)$ uncovered, and each of them must be covered by a codeword of $\mathcal{C}_{d+1}$. In search of the size of $|\mathcal{C}_{d+1}|$, we count the number of pairs (U, V) with $U \in \mathcal{G}_q(n, e+2)$ and $V \in \mathcal{C}_{d+1}$ such that $U \subseteq V$. Double counting gives us

$$\left(\begin{bmatrix} n \\ e+2 \end{bmatrix} - |\mathcal{C}_d| \cdot \begin{bmatrix} d \\ e+2 \end{bmatrix} \right) \cdot 1 = |\mathcal{C}_{d+1}| \cdot \begin{bmatrix} d+1 \\ e+2 \end{bmatrix},$$

which implies that

$$\begin{aligned} |\mathcal{C}_{d+1}| &= \frac{\begin{bmatrix} n \\ e+2 \end{bmatrix} - |\mathcal{C}_d| \cdot \begin{bmatrix} d \\ e+2 \end{bmatrix}}{\begin{bmatrix} d+1 \\ e+2 \end{bmatrix}} \\ &= \frac{\frac{(q^n-1)\cdots(q^{n-e-1}-1)}{(q^{e+2}-1)\cdots(q-1)} - \frac{(q^n-1)\cdots(q^{n-e}-1)}{(q^{2e+1}-1)\cdots(q^{e+1}-1)} \cdot \frac{(q^{2e+1}-1)\cdots(q^e-1)}{(q^{e+2}-1)\cdots(q-1)}}{\frac{(q^{2e+2}-1)\cdots(q^{e+1}-1)}{(q^{e+2}-1)\cdots(q-1)}} \\ &= \frac{(q^n-1)\cdots(q^{n-e}-1)}{(q^{2e+2}-1)\cdots(q^{e+1}-1)} \cdot \left(q^{n-e-1}-1-q^e+1\right). \end{aligned}$$

[3] In Chapter 4 we will define a Steiner structure $\mathscr{S}_q(t,k,n)$ as a subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,t)$ is contained in exactly one subspace of $\mathcal{S}$.

[4] This also follows from Theorem 4.1.6, where the size of a Steiner structure $\mathscr{S}_q(t,k,n)$ is given.

For two elements $V, V' \in \mathcal{C}_{d+1}$ the distance is $d(V, V') \geqslant 2(d+1) - (d+1) = d+1$, so $\mathcal{C}_{d+1}$ is an $(n, M, d+1, d+1)$-code. This implies the inequality

$$\mathcal{A}_q(n, d+1, d+1) \geqslant |\mathcal{C}_{d+1}| = \frac{(q^n-1)\cdots(q^{n-e}-1)}{(q^{2e+2}-1)\cdots(q^{e+1}-1)} \cdot \left(q^{n-e-1} - q^e\right). \tag{3.3.3}$$

Now, applying Theorem 3.1.19 iteratively $e+1$ times, starting with $\mathcal{A}_q(n, d+1, d+1)$, we get

$$\begin{aligned}
\mathcal{A}_q(n, d+1, d+1) &= \mathcal{A}_q(n, 2e+2, 2e+2) \\
&\leqslant \frac{q^n-1}{q^{2e+2}-1}\mathcal{A}_q(n-1, 2e+2, 2e+1) \\
&\leqslant \cdots \\
&\leqslant \frac{(q^n-1)\cdots(q^{n-e}-1)}{(q^{2e+2}-1)\cdots(q^{e+2}-1)} \cdot \mathcal{A}_q(n-(e+1), 2e+2, 2e+2-(e+1)).
\end{aligned} \tag{3.3.4}$$

Combining the upper bound (3.3.4) and the lower bound (3.3.3) for $\mathcal{A}_q(n, d+1, d+1)$, gives us

$$\mathcal{A}_q(n-(e+1), 2e+2, e+1) \geqslant \frac{1}{q^{e+1}-1} \cdot \left(q^{n-e-1} - q^e\right) = q^e \cdot \frac{q^{n-2e-1}-1}{q^{e+1}-1}$$

or, if we write $m = n-(e+1)$ and $k = e+1$,

$$\mathcal{A}_q(m, 2k, k) \geqslant \frac{q^m - q^{k-1}}{q^k - 1} = q^{k-1} \cdot \frac{q^{m-k+1}-1}{q^k-1}.$$

We already observed that $\mathcal{C}_d$ is a Steiner structure $\mathscr{S}_q(e+1, d, n)$. Applying Corollary 4.2.2[5] for parameter $i = e$, gives us the condition that $\begin{bmatrix} d-e \\ 1 \end{bmatrix}$ has to divide $\begin{bmatrix} n-e \\ 1 \end{bmatrix}$, so $\frac{q^{d-e}-1}{q-1}$ has to divide $\frac{q^{n-e}-1}{q-1}$ or equivalently[6] $d-e = e+1 = k$ has to divide $n-e = m+1$.

Using (3.3.1) and the just mentioned fact that k divides $m+1$, we get

$$\begin{aligned}
q^{k-1} \cdot \frac{q^{m-k+1}-1}{q^k-1} &= q^{k-1} \cdot \left(q^{m-2k+1} + q^{m-3k+1} + \cdots + 1\right) \\
&= q^{m-k} + q^{m-2k} + \cdots + q^{k-1} \\
&= \left\lfloor \frac{q^m-1}{q^k-1} \right\rfloor,
\end{aligned}$$

which implies the inequality

$$\mathcal{A}_q(m, 2k, k) \geqslant \left\lfloor \frac{q^m-1}{q^k-1} \right\rfloor. \tag{3.3.5}$$

[5] This is proved independently from this theorem, so we can use it here.
[6] This argument is also discussed in Section 4.2, i.e. below Corollary 4.2.2.

Since $k = e + 1$ divides $m + 1$, it cannot divide m, so $m \not\equiv 0 \pmod{k}$. Therefore (3.3.5) is in contradiction with Lemma 3.3.5.

Case 2. $\{0\} \notin \mathcal{C}$.

In the proof of this case, we will construct a certain partition of $\mathbb{F}_q^n$ and then apply a counting argument to this partition in order to obtain a contradiction.

For the counting argument, we introduce a function η from subsets of $\mathbb{F}_q^n$ to $\mathbb{N}$. This function sends a set $\mathcal{S} \subseteq \mathbb{F}_q^n$ to the value $\eta(\mathcal{S})$, which denotes the number of vectors $(x_1, x_2, \ldots, x_n)$ in $\mathcal{S}$ such that $x_1 = 1$. If $\mathcal{S}$ is a vector space of dimension i and if moreover $\eta(\mathcal{S}) \neq 0$, then $\mathcal{S}$ intersects the hyperplane $X_1 = 0$ in an $(i-1)$-dimensional subspace which consists of q^{i-1} vectors. There remain $q^i - q^{i-1} = q^{i-1}(q-1)$ vectors in $\mathcal{S}$ with a nonzero first coordinate. Since $\mathcal{S}$ is a vector space, to obtain the vectors with $x_1 = 1$, we have to divide by $|\mathbb{F}_q \backslash \{0\}|$, and so we get $\eta(\mathcal{S}) = q^{i-1}$.

Now, let $X \in \mathcal{C}$ be a vector space of the smallest dimension among all the vector spaces in $\mathcal{C}$. Since we are in Case 2, $X \neq \{0\}$ and so we can assume that $\eta(X) \neq 0$, if necessary by permuting the coordinates of the ambient space $\mathbb{F}_q^n$. Let $k = \dim(X)$. In order to construct a partition of $\mathbb{F}_q^n$, we want that the sphere with radius e around X covers the null-space $\{0\}$, and so $k \leqslant e$. Also note that $n > e$, otherwise, $\mathcal{C}$ would be a trivial perfect code. Now consider the hyperplane of all vectors with $x_1 = 0$. Since $\eta(X) \neq 0$, X cannot be contained in the hyperplane $X_1 = 0$, so the dimension of the intersection of this hyperplane with X is $k - 1$. Therefore, we can find a vector space V of dimension $e - k$ in the hyperplane $X_1 = 0$, which intersects trivially with X. Consequently, there are no vectors in V with $x_1 = 1$, so $\eta(V) = 0$. Furthermore, define the vector space $W \coloneqq X \oplus V$. Because of the construction of V, we have $\dim(W) = e$, and since $\eta(X) \neq 0$, it follows that $\eta(W) = q^{e-1}$.

Let us now define a subcode $\mathcal{C}'$ of $\mathcal{C}$ in the following way:

$$\mathcal{C}' \coloneqq \{Y \in \mathcal{C} | V \subset Y \text{ and } \dim(Y) = d - k\}.$$

Suppose that $\mathcal{C}'$ contains M codewords $Y_1, Y_2, \ldots, Y_M$. For all $i = 1, \ldots, M$, let us define $Y_i^* = Y_i \backslash V$. We now claim that these sets Y_i^*, together with W, form a partition of $\mathbb{F}_q^n$. Assume now that

$$Y_1^* \cup Y_2^* \cup \cdots \cup Y_M^* \cup W \tag{3.3.6}$$

is indeed a partition of $\mathbb{F}_q^n$ (we will prove this later on). Since $\dim(Y_i) = d - k$ and $\eta(V) = 0$, it follows that $\eta(Y_i^*) = \eta(Y_i)$ is either 0 or $q^{d-k-1} = q^{2e-k}$ for all i. Furthermore $\eta(\mathbb{F}_q^n) = q^{n-1}$ and hence,

$$\eta(W) = \eta(\mathbb{F}_q^n) - \sum_{i=1}^{M} \eta(Y_i^*)$$

must be divisible by q^{2e-k}. But, we have already shown that $\eta(W) = q^{e-1}$. But $e - 1 < 2e - k$ for all $k \leqslant e$, so this gives a contradiction.

The only remaining part of the proof of this theorem is that we have to prove that (3.3.6) is indeed a partition of $\mathbb{F}_q^n$. We will first prove that every element of $\mathbb{F}_q^n$ is contained in the set (3.3.6) and that all these sets do not pairwise intersect.

Claim 1. Let u be a vector of $\mathbb{F}_q^n$ that lies outside of W, then there exists a codeword $Y_i \in \mathcal{C}'$ such that $u \in Y_i$.

Proof. Let $U = \langle V, u \rangle$. This vector space U has dimension $e-k+1$ and has to be covered by a sphere $\mathcal{S}_e(Y)$, for some codeword $Y \in \mathcal{C}$. Since $U \cap X = \{0\}$ and therefore

$$d(X, U) = \dim(X) + \dim(U) - 2\dim(X \cap U) = k + (e - k + 1) - 0 = e + 1,$$

this codeword is not X. From the fact that X and Y are distinct codewords of $\mathcal{C}$, we must have $d(X, Y) \geqslant d$. This implies that

$$\dim(Y) = d(X, Y) - \dim(X) + 2\dim(X \cap Y) \geqslant d - k = 2e + 1 - k.$$

Furthermore, we have

$$\begin{aligned} d(U, Y) &= \dim(U) + \dim(Y) - 2\dim(U \cap Y) \\ &\geqslant (e - k + 1) + \dim(Y) - 2(e - k + 1) \\ &\geqslant (2e + 1 - k) - (e - k + 1) \\ &= e. \end{aligned} \tag{3.3.7}$$

On the other hand, since $\mathcal{S}_e(Y)$ covers U, we know that $d(U, Y) \leqslant e$. Therefore, $d(U, Y) = e$ and every inequality in (3.3.7) is an equality, so the only possible value of $\dim(Y)$ is $d - k$. This implies that

$$\dim(U \cap Y) = \frac{1}{2}(\dim(U) + \dim(Y) - d(U, Y)) = \frac{1}{2}(e - k + 1 + d - k - e) = e - k + 1 = \dim(U),$$

from which it follows that $V \subset U \subset Y$ and hence $Y \in \mathcal{C}'$. Finally, from the definition of U, $U \subset Y$ also implies that $u \in Y$, which shows that the claim holds. □

If u is not contained in $W = X \oplus V$ and $u \in Y_i$, then u must belong to $Y_i^* = Y_i \backslash V$. Hence, this first claim shows that every vector is contained in at least one of the sets $Y_1^*, Y_2^*, \cdots, Y_M^*, W$. The next claim guarantees that all vectors are contained in at most one of these sets.

Claim 2. The sets $Y_1^*, Y_2^*, \ldots, Y_M^*$ and W are pairwise disjoint.

Proof. Consider first two different codewords Y_i and Y_j in $\mathcal{C}'$. Since

$$d \leqslant d(Y_i, Y_j) = 2(d - k) - 2\dim(Y_i \cap Y_j),$$

it follows from $d = 2e + 1$ that $\dim(Y_i \cap Y_j) \leqslant e - k = \dim(V)$ and therefore $Y_i \cap Y_j = V$. Consequently, the sets $Y_1^*, Y_2^*, \ldots, Y_M^*$ are pairwise disjoint.

Now assume to the contrary that there exists a nonzero vector y in the intersection $Y_i^* \cap W$ for some i. Then $y \in Y_i$, and $y = x + v$ for some nonzero $x \in X$ and some $v \in V$. But Y_i is a vector space which contains the subspace V. Therefore Y_i also contains the vector $y - v = x$, and so $\dim(X \cap Y_i) \geqslant 1$. But on the other hand,

$$d \leqslant d(X, Y_i) = k + (d - k) - 2\dim(X \cap Y_i) \leqslant d - 2,$$

which is clearly a contradiction. □

The proof of these two claims completes the proof of Case 2. Now we have indeed shown that there are no nontrivial perfect codes in $\mathcal{P}_q(n)$. □

Chapter 4

Designs over $\mathbb{F}_q$

A ***t*-(n, k, λ) *q-design*** over $\mathbb{F}_q$ is a set $\mathcal{S}$ of k-dimensional subspaces of the n-dimensional vector space $\mathbb{F}_q^n$ such that each t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly λ elements of $\mathcal{S}$. This is the q-analogue of the t-(n, k, λ) design defined in Definition 1.2.1. Also the Steiner systems, i.e. designs with parameters t-$(n, k, 1)$, have a q-analogue. These will be called ***q-Steiner systems*** or ***Steiner structures***. In geometrical terms, a Steiner structure $\mathscr{S}_q(t, k, n)$ is called a ***(t, k)-spread***. In this chapter we are amongst other things interested in the existence of these Steiner structures. For example, Steiner structures with $t = 1$ are known as ***spreads*** and exist if and only if k divides n. In Chapter 5 we will explore these structures more in detail and link this with (partial) spread codes. We will also discuss the recent result in [5] of the existence of a Steiner structure $\mathscr{S}_2(2, 3, 13)$.

Furthermore, this chapter discusses two other designs. A Steiner structure $\mathscr{S}_q(t, k, n)$ is a subset $\mathcal{S}$ such that each element $U \in \mathcal{G}_q(n, k)$ is contained in exactly one subspace of $\mathcal{S}$. In a ***q-covering design*** this element U 'only' has to be contained in at least one subspace of $\mathcal{S}$. Also the dual notion, a ***q-Turán design***, is considered. Along with some elementary properties in Section 4.1, some upper and lower bounds will be discussed. For some specific parameters (see e.g. in Subsection 4.4.1) this leads to exact values for q-covering numbers.

We base our study here on the investigation of Schwartz and Etzion in [34], of Etzion and Vardy in [18] and of Braun and Wassermann in [5].

4.1 Covering designs, Steiner structures and Turán designs

In this section, we consider the q-analogues of covering designs, Steiner systems and Turán designs, as defined in Subsection 1.2. We will assume that the ambient space $\mathcal{W}$ is $\mathbb{F}_q^n$, but we want to point out that these results are valid for an arbitrary n-dimensional vector space over $\mathbb{F}_q$.

Definition 4.1.1. A ***q-covering design*** $\mathscr{C}_q(n,k,t)$ is a subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,t)$ is contained in at least one subspace of $\mathcal{S}$. The ***q-covering number*** $\mathcal{C}_q(n,k,t)$ is the minimum size of a q-covering design $\mathscr{C}_q(n,k,t)$.

Definition 4.1.2. A ***Steiner structure*** $\mathscr{S}_q(t,k,n)$[1] is a subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,t)$ is contained in exactly one subspace of $\mathcal{S}$.

A Steiner structure $\mathscr{S}_q(t,k,n)$, when it exists, is the smallest q-covering design $\mathscr{C}_q(n,k,t)$.

Definition 4.1.3. A ***q-Turán design*** $\mathscr{T}_q(n,k,t)$ is a subset $\mathcal{S}$ of $\mathcal{G}_q(n,t)$ such that each element of $\mathcal{G}_q(n,k)$ contains at least one subspace from $\mathcal{S}$. The ***q-Turán number*** $\mathcal{T}_q(n,k,t)$ is the minimum size of a q-Turán design $\mathscr{T}_q(n,k,t)$.

There is a close relation between these concepts. The following theorem and corollary show that q-covering designs and q-Turán designs are dual objects.

Theorem 4.1.4. *A subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ is a q-covering $\mathcal{C}_q(n,k,t)$ if and only if its orthogonal complement $\mathcal{S}^\perp$ is a q-Turán design $\mathscr{T}_q(n,n-t,n-k)$.*

Proof. Assume first that $\mathcal{S}$ is a q-covering design $\mathscr{C}_q(n,k,t)$. We have to prove that every subspace in $\mathcal{G}_q(n,n-t)$ contains at least one element of $\mathcal{S}^\perp = \{V^\perp \in \mathcal{G}_q(n,n-k) | V \in \mathcal{S}\}$. So take an arbitrary subspace U in $\mathcal{G}_q(n,n-t)$. Then $\dim U^\perp = t$ and, hence, there exists at least one $V \in \mathcal{S}$ such that $U^\perp \subseteq V$. The key to success is the fact that

$$U^\perp \subseteq V \Leftrightarrow V^\perp \subseteq U.$$

Since $V^\perp \in \mathcal{S}^\perp$, this means that U contains at least one element of $\mathcal{S}^\perp$ and this proves the first part of the theorem.

The proof of the necessary condition uses similar arguments. Let $\mathcal{S}$ be a q-Turán design $\mathscr{T}_q(n,n-t,n-k)$ and consider $U \in \mathcal{G}_q(n,t)$, then $U^\perp \in \mathcal{G}_q(n,n-t)$ and it contains a certain $(n-k)$-dimensional subspace V. Again, since $V \subseteq U^\perp$ if and only if $U \subseteq V^\perp$, every subspace U of $\mathcal{G}_q(n,t)$ is contained in at least one subspace of $\mathcal{S}^\perp$, hence $\mathcal{S}^\perp$ is a q-covering design $\mathscr{C}_q(n,k,t)$. □

Corollary 4.1.5.

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

We are also interested in the size of these designs. In particular in Section 4.4, we discuss bounds on the sizes of q-covering designs and q-Turán designs. We already noticed that Steiner structures are special cases of q-covering designs. This connection is also demonstrated in the next theorem, which exhibits a lower bound on $\mathcal{C}_q(n,k,t)$ and gives the size of a Steiner system $\mathscr{S}_q(t,k,n)$, if it exists.

[1] The parameters are a bit confusing, but we want to keep this notation, because of the link with the notation of the classical concepts and also because it is well known in the literature. This is the notation of [18]. A Steiner structure with parameters t,k and n is sometimes denoted as $S_q[t,k,n]$ (see e.g. [5]) or $S[t,k,n]$ (see e.g. [34]).

Theorem 4.1.6. *Let $\mathcal{S}$ be a q-covering design $\mathscr{C}_q(n,k,t)$. Then*

$$|\mathcal{S}| \geqslant \frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}},$$

with equality if and only if $\mathcal{S}$ is a Steiner structure $\mathscr{S}_q(t,k,n)$.

Proof. Every element of $\mathcal{S}$ is a k-dimensional subspace, and therefore contains exactly $\begin{bmatrix} k \\ t \end{bmatrix}$ distinct t-dimensional subspaces. Since the total number of t-dimensional subspaces in $\mathcal{W}$ is $\begin{bmatrix} n \\ t \end{bmatrix}$, we need at least $\frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}$ elements in $\mathcal{S}$ to cover all these t-dimensional subspaces, so

$$|\mathcal{S}| \geqslant \frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}.$$

If $|\mathcal{S}|$ achieves this bound with equality, each t-dimensional subspace has to be contained in exactly one element of $\mathcal{S}$. This means that $\mathcal{S}$ is a Steiner structure $\mathscr{S}_q(t,k,n)$. Furthermore, if $\mathcal{S}$ is a Steiner structure $\mathscr{S}_q(t,k,n)$, the number of elements is

$$\frac{|\mathcal{G}_q(n,k)|}{|\mathcal{G}_q(k,t)|} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}.$$

□

4.2 On the existence of Steiner structures and Steiner systems

It follows from Theorem 4.1.6 that the most interesting q-covering designs are Steiner structures. An important question is for which parameters Steiner structures do exist. Two trivial examples of Steiner structures are $\mathscr{S}_q(t,n,n)$, which consists of one element, i.e. the whole n-dimensional space, and $\mathscr{S}_q(t,t,n)$, for all $t \leqslant n$. In this section, the discussion about the existence of nontrivial Steiner structures and Steiner systems is considered. This has reached a new level since the construction of the Steiner structure $\mathscr{S}_2(2,3,13)$ in [5], which we will discuss in Section 4.3. We will start with some limitations for the existence of Steiner structures on given parameters.

4.2.1 On the existence of nontrivial Steiner structures

Theorem 4.2.1. *If $\mathscr{S}_q(t,k,n)$ exists, with $t \geqslant 2$, then $\mathscr{S}_q(t-1,k-1,n-1)$ exists.*

Proof. Let $\mathcal{S}$ be a Steiner structure $\mathscr{S}_q(t,k,n)$. We can write the ambient space $\mathcal{W}$ as $W_1 \oplus W_{n-1}$, with $W_1 \in \mathcal{G}_q(n,1)$ and $W_{n-1} \in \mathcal{G}_q(n,n-1)$. We define the set $\mathcal{S}'$ as

$$\mathcal{S}' \coloneqq \{U \cap W_{n-1} | U \in \mathcal{S} \text{ and } W_1 \subseteq U\}.$$

We claim that this set $\mathcal{S}'$ is a Steiner structure $\mathscr{S}_q(t-1,k-1,n-1)$. From the definition of $\mathcal{S}'$ every element of this set is contained in W_{n-1}. Since $W_1 \nsubseteq W_{n-1}$, it follows that all elements of $\mathcal{S}'$ are $(k-1)$-dimensional. Furthermore, for each arbitrary $V \in \mathcal{G}_q(n-1,t-1)$, $V \oplus W_1$ is a t-dimensional subspace. Hence, $V \oplus W_1$ is contained in exactly one element $U \in \mathcal{S}$. Therefore, V is contained in exactly one element of $\mathcal{S}'$, i.e. the subspace $U \cap W_{n-1}$. This means that $\mathcal{S}'$ is indeed a Steiner structure $\mathscr{S}_q(t-1,k-1,n-1)$, and the theorem follows. □

Together with Theorem 4.1.6, the previous theorem gives some necessary conditions on the existence of a Steiner structure.

Corollary 4.2.2. *If $\mathscr{S}_q(t,k,n)$ exists, then $\begin{bmatrix} n-i \\ t-i \end{bmatrix} \Big/ \begin{bmatrix} k-i \\ t-i \end{bmatrix}$, for all $0 \leqslant i \leqslant t-1$, must be integers.*

For $t = 1$, the previous corollary implies that the Steiner structure $\mathscr{S}_q(1,k,n)$ exists, only if k divides n. Indeed, assuming that $n = sk+r$, with $0 \leqslant r \leqslant k-1$, it follows that

$$\begin{aligned} \frac{q^n-1}{q^k-1} &= \frac{q^n-q^{n-k}}{q^k-1} + \frac{q^{n-k}-1}{q^k-1} = q^{n-k} + \frac{q^{n-k}-q^{n-2k}}{q^k-1} + \frac{q^{n-2k}-1}{q^k-1} \\ &= q^{n-k} + q^{n-2k} + \ldots + q^{n-sk} + \frac{q^r-1}{q^k-1}, \end{aligned}$$

so $\dfrac{q^n-1}{q^k-1}$ is an integer if and only if $r = 0$.

Furthermore, for every k which divides n, we can construct a Steiner structure $\mathscr{S}_q(1,k,n)$. Let $n = sk$ and let $\xi \in \mathbb{F}_{q^n}$ be a root of a primitive polynomial of degree s over $\mathbb{F}_{q^k}$. Denote

$$r = \frac{q^n-1}{q^k-1} = q^{(s-1)k} + q^{(s-2)k} + \ldots + q^k + 1$$

and for each i, $0 \leqslant i \leqslant r-1$, we define

$$H_i \coloneqq \{\xi^i, \xi^{r+i}, \xi^{2r+i}, \ldots, \xi^{(q^k-2)r+i}\}.$$

If $\xi^{i+lr} = \xi^{j+mr}$, $0 \leqslant l,m \leqslant q^k-2$ and $0 \leqslant i,j \leqslant r-1$, then $i-j+(l-m)r = 0$, since ξ is a primitive root. So every element of $\mathbb{F}_{q^n} \backslash \{0\}$ appears once and only once in a set H_i for some i, $0 \leqslant i \leqslant r-1$. It can also be verified that $H_0 \cup \{0\} = \mathbb{F}_{q^k}$ and that all such H_i, viewed as a set of vectors of length n over $\mathbb{F}_q$, form a partition of $\mathbb{F}_q^n$. Each such set is an element in $\mathscr{S}_q(1,k,n)$. This gives a regular Desarguesian spread.

The observation considered above leads us to the following corollary.

Corollary 4.2.3. *A Steiner structure $\mathscr{S}_q(1,k,n)$ exists if and only if k divides n.*

We already mentioned in the beginning of this chapter that these specific Steiner structures with $t = 1$ are known as ***spreads*** and will be further discussed in Chapter 5.

For a long time, the Steiner structures $\mathscr{S}_q(1, k, n)$ were considered (and conjectured) to be the only nontrivial Steiner structures. In what follows, two intervals in which only trivial Steiner structures exist, are shown.

Theorem 4.2.4. *If there exist Steiner structures $\mathscr{S}_q(t, k, n)$ with $n \leqslant 2k - t$, then these Steiner structures are trivial Steiner structures $\mathscr{S}_q(t, k, k)$.*

Proof. Let $\mathcal{S}$ be a Steiner structure $\mathscr{S}_q(t, k, n)$ with $n \leqslant 2k - t$. Assume U and V are two different elements of $\mathcal{S}$. It follows that $\dim(U \cap V) \leqslant t - 1$ and hence,

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V) \geqslant 2k - t + 1 > n,$$

which is a contradiction. Therefore $\mathcal{S}$ contains at most one element. Since every element of $\mathcal{G}_q(n, t)$ has to be contained in this one k-dimensional element, this means $k = n$. □

Theorem 4.2.5. *If there exist Steiner structures $\mathscr{S}_q(t, k, n)$ with $2k - t < n < 2k$, then these Steiner structures are trivial Steiner structures $\mathscr{S}_q(k, k, n)$.*

Proof. Let $\mathcal{S}$ be a $\mathscr{S}_q(t, k, n)$, with $2k - t < n < 2k$. We will do a double counting on the set

$$S \coloneqq \{(U, V) | U \in \mathcal{S} \text{ and } V \in \mathcal{G}_q(n, 2k - t) \text{ such that } U \subseteq V\}.$$

Each element $U \in \mathcal{S}$ is contained in exactly $\begin{bmatrix} n-k \\ (2k-t)-k \end{bmatrix} = \begin{bmatrix} n-k \\ k-t \end{bmatrix}$ subspaces V of dimension $2k-t$. On the other hand, if two subspaces W_1 and W_2 of dimension k would be contained in a subspace $V \in \mathcal{G}_q(n, 2k - t)$, then $\dim(W_1 + W_2) \leqslant 2k - t$ and so $\dim(W_1 \cap W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 + W_2) \geqslant 2k - (2k - t) = t$. So each $(2k - t)$-dimensional subspace V contains no more than one element of $\mathcal{S}$. Therefore,

$$|S| = \begin{bmatrix} n-k \\ k-t \end{bmatrix} \cdot |\mathcal{S}| = \begin{bmatrix} n-k \\ k-t \end{bmatrix} \frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}} \leqslant |\mathcal{G}_q(n, 2k - t)| = \begin{bmatrix} n \\ 2k-t \end{bmatrix}. \tag{4.2.1}$$

Because of the property that $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$, the inequality of (4.2.1) implies

$$\frac{\begin{bmatrix} n-k \\ k-t \end{bmatrix}}{\begin{bmatrix} k \\ k-t \end{bmatrix}} \cdot \frac{\begin{bmatrix} n \\ n-t \end{bmatrix}}{\begin{bmatrix} n \\ n-2k+t \end{bmatrix}} \leqslant 1,$$

or equivalently, by the definition of the Gaussian coefficient,

$$\frac{(q^{n-k} - 1) \cdots (q^{n-2k+t+1} - 1)}{(q^k - 1) \cdots (q^{t+1} - 1)} \cdot \frac{\frac{(q^n-1)\cdots(q^{t+1}-1)}{(q^{n-t}-1)\cdots(q-1)}}{\frac{(q^n-1)\cdots(q^{2k-t+1}-1)}{(q^{n-2k+t}-1)\cdots(q-1)}} \leqslant 1.$$

$\Leftrightarrow$

$$\frac{(q^{n-k} - 1) \cdots (q - 1) \cdot (q^{n-t} - 1) \cdots (q^{t+1} - 1)}{(q^k - 1) \cdots (q^{t+1} - 1) \cdot (q^{n-t} - 1) \cdots (q - 1) \cdot (q^n - 1) \cdots (q^{2k-t+1} - 1)} \leqslant 1.$$

Since $k \geqslant t$, it follows that $2k - t + 1 \geqslant t + 1$ and we can simplify the inequality above and get

$$\frac{(q^{n-k}-1)\cdots(q-1)\cdot(q^{2k-t}-1)\cdots(q^{t+1}-1)}{(q^k-1)\cdots(q^{t+1}-1)\cdot(q^{n-t}-1)\cdots(q-1)} \leqslant 1.$$

Multiplying the numerator and denominator by $(q^t-1)\cdots(q-1)$ gives us

$$\frac{(q^{n-k}-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)} \cdot \frac{(q^{2k-t}-1)\cdots(q-1)}{(q^{n-t}-1)\cdots(q-1)} \leqslant 1.$$

The assumption that $n < 2k$ implies that $n - k < k$ and $n - t < 2k - t$, so we can eliminate some factors in the numerator and denominator. Replacing the remaining factors in ascending order leads us to

$$\frac{(q^{n-t+1}-1)(q^{n-t+2}-1)\cdots(q^{2k-t}-1)}{(q^{n-k+1}-1)(q^{n-k+2}-1)\cdots(q^k-1)} \leqslant 1. \tag{4.2.2}$$

Now both the numerator and denominator have $2k - n$ factors. Since $k \geqslant t$, we know that $\frac{q^{n-t+i}-1}{q^{n-k+i}-1} \geqslant 1$, for $i = 1, \ldots, 2k-n$. It follows that inequality (4.2.2) can hold only if $k = t$, so we have a trivial Steiner structure. □

Corollary 4.2.6. *If a nontrivial Steiner structure $\mathscr{S}_q(t,k,n)$ exists, then $n \geqslant 2k$.*

4.2.2 Deriving Steiner systems from Steiner structures

Recall that a Steiner system $\mathcal{S}(t,k,n)$ is a collection $\mathcal{S}$ of k-subsets of an n-set such that every t-subset of the n-set is contained in exactly one block of $\mathcal{S}$. We already noticed that Steiner structures are the q-analogues of Steiner systems. Another link between these concepts is established in Theorem 4.2.8 (based on [34]), which uses the next theorem. It is a tool to obtain new Steiner systems from Steiner structures, using linear codes.

Theorem 4.2.7. *Let $\mathcal{S}$ be a Steiner structure $\mathscr{S}_q(t,k,r)$ and let H be the set of column vectors of the $r \times n$ parity-check matrix of an $[n,k',d]$-code over $\mathbb{F}_q$, where $r = n - k'$ and $d - 1 \geqslant t$. If there exists an integer $v \geqslant t$ such that the set*

$$\mathcal{S}' \coloneqq \{U \cap H \,|\, U \in \mathcal{S} \text{ and } |U \cap H| \geqslant t\}$$

is a collection of v-subsets of H, then $\mathcal{S}'$ is a Steiner system $\mathcal{S}(t,v,n)$.

Proof. By the fundamental theorem (see Theorem 1.1.25), every $d-1$ columns in the parity-check matrix of an $[n,k',d]$-code are linearly independent. Consequently, the span of each set of t columns from H forms a t-dimensional subspace, which is contained in exactly one element of $\mathcal{S}$, so these t vectors are also contained in exactly one block of $\mathcal{S}'$. Since all the elements of $\mathcal{S}'$ are v-subsets of the n-set H, it follows that $\mathcal{S}'$ is a Steiner system $\mathcal{S}(t,v,n)$. □

Using Theorem 4.2.7 with Hamming codes, we obtain the following theorem.

Theorem 4.2.8. *The existence of a Steiner structure $\mathscr{S}_q(2,k,n)$ implies the existence of Steiner systems $\mathcal{S}(2,\frac{q^k-1}{q-1},\frac{q^n-1}{q-1})$ and $\mathcal{S}(2,q^{k-1},q^{n-1})$. Furthermore, the existence of $\mathscr{S}_2(3,k,n)$ implies the existence of a Steiner system $\mathcal{S}(3,2^{k-1},2^{n-1})$.*

Proof. If we take H to be the set of columns of the parity-check matrix of the linear $[\frac{q^n-1}{q-1},\frac{q^n-1}{q-1}-n,3]$-code, so the Hamming code $\mathrm{Ham}(n,q)$, we have for every element U of a Steiner structure $\mathscr{S}_q(2,k,n)$ with $|U\cap H|\geqslant 2$, the same size of $U\cap H$, so $v=|U\cap H|=\frac{q^k-1}{q-1}$, since all vector lines of a k-dimensional vector subspace have one representative as column in the parity-check matrix. It follows from Theorem 4.2.7 that a Steiner structure $\mathcal{S}(2,\frac{q^k-1}{q-1},\frac{q^n-1}{q-1})$ exists.

Let H be the set of columns from the parity-check matrix of the $[q^{n-1},q^{n-1}-n,d]$-code over $\mathbb{F}_q$, with $d\geqslant 3$, whose columns consist of all the vectors of length n ending with a 1. Since the affine part of every subspace $U\in\mathcal{G}_q(n,k)$ consists of exactly q^{k-1} vectors ending with a 1, the existence of $\mathscr{S}_q(2,k,n)$ implies, using Theorem 4.2.7, the existence of $\mathcal{S}(2,q^{k-1},q^{n-1})$.

Finally, we take H to be the set of columns from the parity-check matrix of the linear $[2^{n-1},2^{n-1}-n,4]$-code, i.e. the binary extended Hamming code $\widehat{\mathrm{Ham}}(n-1,2)$. Again by Theorem 4.2.7, we find that the existence of $\mathcal{S}(3,2^{k-1},2^{n-1})$ follows from the existence of $\mathscr{S}_2(3,k,n)$. □

This theorem gives in a sense a limitation on the existence of Steiner structures $\mathscr{S}_q(t,k,n)$. Nevertheless, Steiner systems of strength 2 seem not that rare, there are numerous Steiner systems $\mathcal{S}(2,2^{k-1},2^{n-1})$ and $\mathcal{S}(2,2^k-1,2^n-1)$ (see e.g. [8]). However, the next theorem, proved in [18], shows that constructing $\mathscr{S}_2(2,k,n)$ is likely to be much harder than what Theorem 4.2.8 suggests.

Theorem 4.2.9. *The existence of a Steiner structure $\mathscr{S}_2(2,k,n)$ implies the existence of a Steiner system $\mathcal{S}(3,2^k,2^n)$.*

Proof. Let $\mathcal{S}$ be a Steiner structure $\mathscr{S}_2(2,k,n)$. Each subspace of $\mathcal{S}$ partitions $\mathbb{F}_2^n$ into $\frac{2^n}{2^k}=2^{n-k}$ additive translates of itself. All such translates form the set

$$\mathcal{S}' := \{\{u,u+v_1,u+v_2,\ldots,u+v_{2^k-1}\}|\{0,v_1,\ldots,v_{2^k-1}\}\in\mathcal{S} \text{ and } u\in\mathbb{F}_2^n\}\,.$$

We will prove that $\mathcal{S}'$ is a Steiner system $\mathcal{S}(3,2^k,2^n)$. First notice that the size of $\mathcal{S}'$ is already exactly $|\mathcal{S}(3,2^k,2^n)|$, because

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

This means that to complete the proof, it is sufficient to prove that every subset $\{x,y,z\}$ of 3 elements of $\mathbb{F}_2^n$ is contained in some block of $\mathcal{S}'$. Since $\mathcal{S}$ is a Steiner structure $\mathcal{S}_2(2,k,n)$, the two-dimensional subspace $\{0,x+y,x+z,y+z\}$ is contained in some k-dimensional subspace V of $\mathcal{S}$. From the definition of $\mathcal{S}'$, it follows that $x+V$ is a block of $\mathcal{S}'$. But $x+\{0,x+y,x+z,y+z\}=\{x,y,z,x+y+z\}$ and therefore the subset $\{x,y,z\}$ is contained in the 2^k-set $x+V$. □

Numerous efforts were made to find Steiner systems of the form $\mathcal{S}(3, 2^k, 2^n)$ (see e.g. [18] and [19]). Because of the existence of the trivial $\mathscr{S}_2(3, 3, n)$ for all $n \geqslant 3$, it follows from Theorem 4.2.8 that the Steiner system $\mathcal{S}(3, 4, 2^{n-1})$ exists, for all $n \geqslant 3$. Nevertheless, the case where $2^k \geqslant 8$ is much harder. Theorem 4.2.9 implies that constructing a Steiner structure $\mathscr{S}_2(2, k, n)$, if such structures exist at all, would be very difficult too. Furthermore, some people conjectured or were tempted to conjecture that they do not exist.

In the search for more nontrivial Steiner structures $\mathscr{S}_2(2, k, n)$, it is natural to start with those of the form $\mathscr{S}_2(2, 3, n)$. First, note that because of Corollary 4.2.2,

$$\frac{\begin{bmatrix} n \\ 2 \end{bmatrix}_2}{\begin{bmatrix} 3 \\ 2 \end{bmatrix}_2} = \frac{(2^n - 1)(2^{n-1} - 1)}{(2^3 - 1)(2^2 - 1)}$$

and

$$\frac{\begin{bmatrix} n-1 \\ 1 \end{bmatrix}_2}{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_2} = \frac{2^{n-1} - 1}{2^2 - 1}$$

have to be integers. The last condition means that 2 has to divide $n - 1$ (see also the argumentation below Corollary 4.2.2) and consequently, 3 has to divide n or $n - 1$. So it follows that

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 0 \pmod 3 \end{cases} \quad \text{or} \quad \begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 1 \pmod 3 \end{cases} \tag{4.2.3}$$

or equivalently, by the Chinese remainder theorem,

$$n \equiv 3 \pmod 6 \quad \text{or} \quad n \equiv 1 \pmod 6.$$

So the first interesting Steiner structures to consider are $\mathscr{S}_2(2, 3, 7)$, $\mathscr{S}_2(2, 3, 9)$ and $\mathscr{S}_2(2, 3, 13)$. Until now, no Steiner structures $\mathscr{S}_2(2, 3, 7)$ or, related by Theorem 4.2.9, no Steiner systems $\mathcal{S}(3, 8, 128)$ have been found. There is also no prove of the existence or nonexistence of Steiner structures $\mathscr{S}_2(2, 3, 9)$. However, next to the spreads $\mathscr{S}_q(1, k, n)$, there do exist nontrivial Steiner structures, which is recently proved in [5]. In the next section, we discuss the construction of the Steiner system $\mathscr{S}_2(2, 3, 13)$.

4.3 On the existence of Steiner structures $\mathscr{S}_2(2, 3, 13)$ and Steiner systems $\mathcal{S}(3, 8, 8192)$

In the beginning of this chapter, we already observed that a Steiner structure is a special case of a t-(n, k, λ) q-design with $\lambda = 1$. Of all the known t-(n, k, λ) q-designs, the design with the largest value for t is a 3-$(8, 4, 12)$ 2-design. In [4], Braun, Kerber and Lauen found this by using a promising method. This 3-$(8, 4, 12)$ 2-design, and also other

known t-(n,k,λ) q-designs, were constructed with the Kramer-Mesner method ([27]) using as group of automorphisms the normalizer of a Singer cycle. This method will also be very useful to construct a 2-$(13,3,1)$ 2-design, also known as a Steiner structure $\mathscr{S}_2(2,3,13)$. This construction is very important, since this is the first construction of a Steiner structure $\mathscr{S}_q(t,k,n)$ with $t > 1$, which implies that there do exist such Steiner structures, despite of all the previous conjectures about the nonexistence of these structures, nontrivial q-Steiner systems which are no spreads. In this subsection, we first explain the Kramer-Mesner method and the Singer cycle and we then use these concepts for the construction of $\mathscr{S}_2(2,3,13)$, based on the recent preprint [5] of Braun and Wassermann.

4.3.1 Kramer-Mesner method

In order to construct a Steiner structure $\mathscr{S}_2(2,3,13)$ using the Kramer-Mesner method, we will give some insightful examples.

Example 4.3.1. An ovoid $\mathcal{O}$ is a subset of points on the parabolic quadric $Q(4,q)$ (see e.g. [23] or [33] for more information) such that every line of $Q(4,q)$ contains exactly one point of $\mathcal{O}$. Consider now the incidence matrix A where the indices[2] i of the rows correspond with the lines L_i of $Q(4,q)$ and the indices j of the columns correspond with the points p_j of $Q(4,q)$. Therefore $A_{ij} = 1$ if $p_j \in L_i$ and $A_{ij} = 0$ if $p_j \notin L_i$. Since $|Q(4,q)| = \frac{q^4-1}{q-1} = q^3+q^2+q+1$ and this value is also the number of generators of $Q(4,q)$, which are lines in this case, the matrix A is a square matrix of order q^3+q^2+q+1. Denote x to be a vector of length q^3+q^2+q+1, with coordinates $x_i \in \{0,1\}$, which is the characteristic vector of $\mathcal{O}$. This means that $x_i = 1$ if the i-th point of $Q(4,q)$ is an element of $\mathcal{O}$ and $x_i = 0$ if not. Then we have

$$A \cdot x = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}. \tag{4.3.1}$$

Indeed, (4.3.1) is equivalent to

$$\sum_j A_{ij} \cdot x_j = 1, \qquad \forall i \in \{1, \ldots, q^3+q^2+q+1\},$$

and since $A_{ij} \in \{0,1\}$ for all i,j, if $\sum_j A_{ij} \cdot x_j = 1$, it follows that, for a fixed index i, there is just one j such that $A_{ij}\dot{x}_j = 1$. This corresponds to the unique element $p_j \in \mathcal{O}$ on the line L_i.

On the other hand, if we construct an incidence matrix for the lines and points of $Q(4,q)$, every 0-1-solution x of the equations (4.3.1) will also correspond to an ovoid of $Q(4,q)$. This technique will be used to find Steiner structures.

Example 4.3.2. A Steiner structure $\mathscr{S}_2(2,3,13)$ can be seen as a set $\mathcal{S}$ of planes in the projective space $\mathrm{PG}(12,2)$, such that every line is contained in exactly one element

[2] The order of the indices can be taken arbitrarily, but once this is chosen, it has to be fixed.

of $\mathcal{S}$. The incidence matrix A is now defined as the matrix with entries A_{ij} such that $A_{ij} = 1$ if the line L_i is contained in the plane β_j and $A_{ij} = 0$ if L_i is not contained in β_j. Note that the objects that have to be taken for the required set, are the elements corresponding with the columns. Now, a Steiner structure $\mathscr{S}_2(2, 3, 13)$, if it exists, would correspond to a 0-1-solution x of (4.3.1). Namely, take the subset $\mathcal{S}$ of all planes β_j such that the index j corresponds to a nonzero element on position j in the characteric vector x. Then, for an arbitrary line L_i for some index i, there is exactly one plane β_j which covers L_i, since there is only one unique j such that $A_{ij} \cdot x_j = 1$. This follows from the fact that for a fixed i, $\sum_j A_{ij} \cdot x_j = 1$ and $A_{ij} \geqslant 0$, so there has to be exactly one j such that $A_{ij} \cdot x_j = 1$ and $A_{ik} \cdot x_k = 0$, for $k \neq j$. This argumentation indeed implies that the subset $\mathcal{S}$ would be a Steiner structure $\mathscr{S}_2(2, 3, 13)$.

In the more general case of a t-(n, k, λ) q-design, consider the incidence matrix $A_{t,k}$, where the rows correspond to a t-subspace $T \in \mathcal{G}_q(n, t)$ and where the columns correspond to a k-subspace $K \in \mathcal{G}_q(n, k)$. The entries $a_{T,K}$ of the matrix $A_{t,k}$ are defined as follows:

$$a_{T,K} \coloneqq \begin{cases} 1 & \text{if } T \subseteq K \\ 0 & \text{otherwise.} \end{cases} \tag{4.3.2}$$

Then in [4], the following corollary is stated.

Corollary 4.3.3. *The set of t-(n, k, λ) q-designs on $\mathbb{F}_q^n$ is the set of selections of k-subspaces that can be obtained from the 0-1-solutions x of the system of linear equations*

$$A_{t,k} \cdot x = \begin{bmatrix} \lambda \\ \vdots \\ \lambda \end{bmatrix},$$

where the components of x are indexed by all k-subspaces K of $\mathbb{F}_q^n$. The set $\mathcal{S}$ of blocks K of the design corresponding to the solution x is

$$\mathcal{S} \coloneqq \{K \in \mathcal{G}_q(n, k) |\, x_K = 1\}.$$

Since the number of lines in $PG(12, 2)$ is $\frac{(2^{13}-1)(2^{12}-1)}{3} = 11180715$ and the number of planes in $PG(12, 2)$ is $\frac{(2^{13}-1)(2^{12}-1)(2^{11}-1)}{(2^3-1)(2^2-1)(2-1)} = 3269560515$, it is clear that the incidence matrix $A_{2,3}$, defined in Example 4.3.2, is a $(11180715 \times 3269560515)$-matrix. Solving the equations of the linear system

$$A_{2,3} \cdot x = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

to obtain a Steiner structure $\mathscr{S}_2(2, 3, 13)$, is, to say the least, really hard. For the same reason, Corollary 4.3.3 is not very useful from the computational point of view, except maybe for some smaller examples. Therefore, we want to reduce the size of the matrix by using a group of automorphisms.

An ***automorphism*** of a t-(n,k,λ) q-design $\mathcal{S}$ is an element ϕ of the general linear group $\mathrm{GL}(n,q)$ which leaves the design invariant, i.e. it maps blocks into blocks. In fact, it just permutes the design, so

$$\{\phi(K)|K \in \mathcal{S}\} = \mathcal{S}.$$

Also the inclusion of t-dimensional subspaces T in subspaces K of dimension k is invariant under the action of the automorphism, i.e.

$$T \subseteq K \Rightarrow \phi(T) \subseteq \phi(K).$$

Therefore, for every $T \in \mathcal{G}_q(n,t)$ and every $K \in \mathcal{G}_q(n,k)$, the number of k-subspaces K' in the orbit of K which covers T is constant on the orbit of T.

A group consisting only of automorphisms of $\mathcal{S}$ is an automorphism group of $\mathcal{S}$, the maximal group with this property is called ***the automorphism group*** of $\mathcal{S}$.

For a certain group $G \leqslant \mathrm{GL}(n,q)$ of automorphisms, consider now the G-incidence matrix $A^G_{t,k}$ between the G-orbits on t-subspaces and G-orbits on k-subspaces. The row of the entry $a^G_{T,K}$ of $A^G_{t,k}$ corresponds to the orbit with representative T under the action of G and the column of $a^G_{T,K}$ corresponds to the G-orbit with representative K. This entry $a^G_{T,K}$ gives the number of k-dimensional subspaces in the orbit of K containing the subspace T. This number is the same as the number of k-subspaces in the orbit of K containing another t-subspace T' in the orbit of the representative T, because of the definition of an automorphism. We will use this incidence matrix $A^G_{t,k}$ to find a t-(n,k,λ) q-design similar to the method of Corollary 4.3.3, but with a matrix with smaller dimensions. The Kramer-Mesner method is the procedure which follows from the next theorem.

Theorem 4.3.4. *The set of t-(n,k,λ) q-designs $\mathcal{S}$ on $\mathbb{F}_q^n$ having $G \leqslant \mathrm{GL}(n,q)$ as an automorphism group, can be obtained from the 0-1-vectors solving the linear system of equations*

$$A^G_{t,k} \cdot x = \begin{bmatrix} \lambda \\ \vdots \\ \lambda \end{bmatrix}$$

in the following way:

$$\mathcal{S} := \bigcup_{K:x_K=1} K^G,$$

where K^G is the orbit of K under the automorphism group G.

In the case of the construction of Steiner structures $\mathscr{S}_2(2,3,13)$ we will look to the orbits of the projective lines T and projective planes K in $PG(12,2)$ under a certain group G of automorphisms. The goal is to find solutions of the system

$$A^G_{2,3} \cdot x = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}, \tag{4.3.3}$$

where the incidence matirx $A^G_{2,3}$ is defined as above, i.e. $a^G_{T,K}$ is the number of projective planes in the orbit of K which contain the projective line T.

If $a^G_{T,K} = 1$ for some T and K, this means that for every line T' in the orbit of the line T, there is one element K' in the orbit of K, such that T' is contained in K'. Therefore, such as in Theorem 4.3.4, if there is a 0-1-solution x of (4.3.3), taking all the 3-subspaces K' in the orbit of every K for which $x_K = 1$, will give us a Steiner structure $\mathscr{S}_2(2, 3, 13)$.

Now the question arises, which group of automorphisms will be useful for this purpose. This will be the normalizer of a Singer cycle, which we will describe in the following subsection.

4.3.2 Singer cycle

In search of the answer to the problem of the existence of Steiner structures $\mathscr{S}_q(t, k, n)$ for small parameters q, t, k, n, Etzion and Vardy concentrated in [19] on the parameter $t = 2$, $k = 3$ and $n = 13$ and constructed a 'near-Steiner structure', a set $\mathcal{S}$ of 14 orbits on 3-dimensional subspaces of $\mathbb{F}_2^{13}$ with respect to the normalizer of the Singer cycle $G \leqslant \mathrm{GL}(13, 2)$ such that each subspace of dimension 2 is contained in at most one element of $\mathcal{S}$. Also in [4] this group of automorphisms was promising for the construction of a 3-$(8, 4, 12)$ 2-design.

A ***Singer cycle*** of $\mathrm{PG}(n-1, q)$ is a transformation α which acts in one orbit on the points of $\mathrm{PG}(n-1, q)$, i.e.

$$\mathrm{PG}(n-1, q) = \{P, \alpha(P), \alpha^2(P), \ldots\},$$

for an arbitrary point P of $\mathrm{PG}(n-1, q)$.

Now, in $\mathrm{PG}(n-1, q)$, consider an $(n \times n)$-matrix A with eigenvalues $\lambda, \lambda^q, \lambda^{q^2}, \ldots, \lambda^{q^{n-1}}$, with $\lambda \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$, λ a primitive element of $\mathbb{F}_{q^n}$. This means that the eigenvalues of A are λ and its conjugates over $\mathbb{F}_q$. Then this matrix defines a Singer cycle of $\mathrm{PG}(n-1, q)$, as we will show below.

Assume that α is defined by A and consider the orbit

$$\{P, \alpha(P), \alpha^2(P), \ldots, \alpha^i(P) = P\}.$$

If $\alpha^i(P) = P$, then $A^i \cdot P = \mu P$, for some $\mu \in \mathbb{F}_q \backslash \{0\}$, which means that μ is an eigenvalue of A^i. This implies that $\mu \in \{\lambda^i, \lambda^{iq}, \ldots, \lambda^{iq^{n-1}}\}$. Since $\lambda \in \mathbb{F}_{q^n}$ is a primitive element, $\lambda^{q^n-1} = 1$ and there is no smaller power of λ with the same property. Furthermore, we have

$$\lambda^{q^n-1} = \left(\lambda^{q^{n-1}+q^{n-2}+\cdots+q+1}\right)^{q-1} = 1.$$

This implies that the smallest value of i is $q^{n-1}+\cdots+q+1 = |\mathrm{PG}(n-1, q)|$ and therefore the orbit of a point P is the whole space $\mathrm{PG}(n-1, q)$ and $|\langle\alpha\rangle| = q^{n-1}+q^{n-2}+\cdots+q+1$.

If you see α as an automorphism in the extended projective space $\mathrm{PG}(n-1, q^n)$, α fixes the projective space $\mathrm{PG}(n-1, q)$ as a projective space and it fixes pointwise n other points of $\mathrm{PG}(n-1, q^n) \backslash \mathrm{PG}(n-1, q)$. These points are the eigenvectors $P', P'^q, \ldots, P'^{q^{n-1}}$ of A corresponding to the n eigenvalues $\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}$. Instead of considering the automorphism group $\langle\alpha\rangle \leqslant \mathrm{GL}(n, q)$, we take the normalizer of the Singer cycle:

$$\begin{aligned} N_{\mathrm{GL}(n,q)}(\langle\alpha\rangle) &= \{g \in \mathrm{GL}(n, q) | g\langle\alpha\rangle g^{-1} = \langle\alpha\rangle\} \\ &= \langle\beta, \alpha\rangle, \end{aligned}$$

with $\beta \in \mathrm{GL}(n,q)$ such that $\beta(P') = P'^q, \beta(P'^q) = P'^{q^2}, \ldots, \beta(P'^{q^{n-1}}) = P'$, which is also called the ***Frobenius automorphism***. One inclusion of the last equality follows from the fact that every element of this group $\langle \beta, \alpha \rangle$ stabilizes the projective space $\mathrm{PG}(n-1,q)$ and the set $\{P', P'^q, \ldots, P'^{q^{n-1}}\}$. The other inclusion is also valid. Furthermore, it follows that

$$|N_{\mathrm{GL}(n,q)}(\langle \alpha \rangle)| = n \cdot |\langle \alpha \rangle| = n \cdot \frac{q^n - 1}{q - 1} \tag{4.3.4}$$

This group of automorphisms will help us to reduce the number of rows and columns of the incidence matrix used for the Kramer-Mesner method, which will lead us to the construction of Steiner structures $\mathscr{S}_2(2,3,13)$.

4.3.3 Construction of $\mathscr{S}_2(2,3,13)$

This section on the construction of Steiner structures $\mathscr{S}_2(2,3,13)$ is based on the article [5] of Braun and Wassermann.

Let $G = \langle F, S \rangle \leqslant \mathrm{GL}(13,2)$ be the normalizer of the Singer cycle, generated by the following two matrices F and S, corresponding to a Frobenius automorphism and a Singer cycle. These matrices are

$$F = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1
\end{bmatrix}$$

and

$$S = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

It follows from (4.3.4) that the order of G is $13 \cdot (2^{13} - 1) = 106483$. If there would be a solution x of (4.3.3), with this specific G, every orbit of 3-subspaces has size 106483. From Theorem 4.1.6, it follows that the size of a Steiner structure $\mathscr{S}_2(2, 3, 13)$ is

$$\frac{\begin{bmatrix} 13 \\ 3 \end{bmatrix}_2}{\begin{bmatrix} 13 \\ 2 \end{bmatrix}_2} = \frac{(2^{13} - 1)(2^{12} - 1)}{(2^3 - 1)(2^2 - 1)} = 1597245.$$

Therefore, we require $\frac{1597245}{106483} = 15$ orbits of 3-subspaces under G to obtain such a Steiner structure. Note again that Etzion and Vardy found already in [19] a near-Steiner structure of 14 orbits such that each subspace of dimension 2 is contained in at most one element of these orbits, using the normalizer of the Singer cycle.

In order to apply the Kramer-Mesner method, we need to construct the incidence matrix $A_{2,3}^G$ between orbits of 2-subspaces T and orbits of 3-subspaces K. In [5], it is stated that this matrix has 105 rows and 25572 columns whose entries are all 0 or 1. Note that this strongly reduces the original $(11180715 \times 3269560515)$-incidence matrix. With the dancing links algorithm by D. Knuth [26] on a standard desktop computer, it was possible to solve the Diophantine linear system (4.3.3) and they found that there are at least 26 solutions which define a Steiner structure $\mathscr{S}_2(2, 3, 13)$. In Table 4.1, one solution of 15 orbit representatives is given (see Table 1 of [5]). The union of all those 15 orbits indeed gives a Steiner structure $\mathscr{S}_2(2, 3, 13)$ of $15 \cdot 106483 = 1597245$ elements. From Theorem 4.2.9, we also get the existence of Steiner systems $\mathcal{S}(3, 8, 8192)$.

To conclude this section, we summarize this important result in the following theorem.

Theorem 4.3.5. *Steiner structures* $\mathscr{S}_2(2, 3, 13)$ *and Steiner systems* $\mathcal{S}(3, 8, 8192)$ *do exist.*

$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\0&0&0\\0&0&0\\0&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&1&0\\0&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\0&1&0\\1&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\0&0&0\\1&0&0\\0&1&0\\1&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\\0&1&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$\begin{bmatrix}0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\0&1&0\\0&1&0\\0&1&0\\1&1&0\\1&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\1&0&0\\0&1&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\0&1&0\\0&0&0\\1&0&0\\0&0&0\\0&0&0\\0&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\1&0&0\\1&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\0&1&0\\0&0&0\\0&0&0\\1&1&0\\0&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\\1&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\0&1&0\\0&0&0\\0&1&0\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$\begin{bmatrix}0&0&0\\1&0&0\\0&0&0\\1&0&0\\1&0&0\\1&0&0\\0&1&0\\0&0&0\\1&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}1&0&0\\0&0&0\\1&0&0\\1&0&0\\1&0&0\\1&0&0\\0&1&0\\0&0&0\\1&1&0\\0&0&0\\1&0&0\\1&1&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}1&0&0\\0&0&0\\1&0&0\\1&0&0\\1&0&0\\1&0&0\\0&1&0\\0&0&0\\1&1&0\\0&1&0\\0&0&0\\1&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\0&0&0\\1&0&0\\0&1&0\\0&0&0\\1&1&0\\1&0&0\\0&0&0\\0&0&1\end{bmatrix}\quad\begin{bmatrix}0&0&0\\1&0&0\\1&0&0\\0&0&0\\0&0&0\\0&1&0\\0&0&0\\0&1&0\\1&0&0\\0&1&0\\1&0&0\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

Table 4.1: The 15 orbit representatives of $\mathscr{S}_2(2,3,13)$

4.4 Bounds on q-covering numbers

If a Steiner structure $\mathscr{S}_q(t,k,n)$ exists for given parameters, it follows from Theorem 4.1.6 that $\mathcal{C}_q(n,k,t) = |\mathscr{S}_q(t,k,n)|$. But it is clear from the discussions above that Steiner structures $\mathscr{S}_q(t,k,n)$ do not always exist and if they exist, it is hard to prove it. For a lot of specific parameters, the existence of such Steiner structures is still an open problem. In this section, we want to reduce the interval of the possibilities for the q-covering numbers $\mathcal{C}_q(n,k,t)$. In Subsection 4.4.2 and Subsection 4.4.3, upper and lower bounds on q-covering numbers are established for general parameters q, n, k and t. But first, we give the exact values of $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,t)$, results shown in [17], making use of the relation with the q-Turán numbers. Also, some techniques and results we discuss in these subsections, will be useful in the next chapter, when we talk about (partial) spread codes.

4.4.1 The q-covering numbers $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,t)$

Lemma 4.4.1.

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

Proof. From Theorem 4.1.6, it follows that a Steiner structure $\mathscr{S}_q(1,k,n)$ is an optimal q-covering design $\mathscr{C}_q(n,k,1)$, with

$$|\mathscr{S}_q(1,k,n)| = \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}}{\begin{bmatrix} k \\ 1 \end{bmatrix}} = \frac{q^n-1}{q^k-1},$$

when it exists. The condition for the existence of $\mathscr{S}_q(1,k,n)$, i.e. that k has to divide n, is stated in Corollary 4.2.3. This proves the lemma. □

Lemma 4.4.2.

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

Proof. We can represent $\mathbb{F}_q^n$ as $W_{n-1} \times \mathbb{F}_q$, for a given $W \in \mathcal{G}_q(n,n-1)$, namely $\mathbb{F}_q^n = \left\{(x,\alpha) | x \in \mathbb{F}_q^{n-1}, \alpha \in \mathbb{F}_q\right\}$. Let $\mathcal{S}$ be a q-covering design $\mathscr{C}_q(n-1,k-1,t)$ in an $(n-1)$-dimensional space W_{n-1}, with $|\mathcal{S}| = \mathcal{C}_q(n-1,k-1,t)$. For each $V \in \mathcal{S}$, we define

$$V' \coloneqq \{(v,\alpha) | v \in V \text{ and } \alpha \in \mathbb{F}_q\}.$$

This subspace V' is a k-dimensional subspace of $\mathbb{F}_q^n = W_{n-1} \times \mathbb{F}_q$. If we coordinatize this approach, we can set $X_n = 0$ to be W_{n-1} and $V' = V \oplus \langle(0,\ldots,0,1)\rangle$, where V is interpret in $\mathbb{F}_q^n$ instead of in $\mathbb{F}_q^{n-1}$. Now denote $\mathcal{S}'$ as the set of all such subspaces V', i.e.

$$\mathcal{S}' \coloneqq \{V' \in \mathcal{G}_q(n,k) | V \in \mathcal{S}\}.$$

It is clear that $|\mathcal{S}'| = |\mathcal{S}|$, so if we can show that this set $\mathcal{S}'$ is a q-covering design $\mathscr{C}_q(n,k,t)$, then the q-covering number $\mathcal{C}_q(n,k,t)$ is at most the size of $\mathcal{S}'$, i.e. $|\mathcal{S}'| = |\mathcal{S}| = \mathcal{C}_q(n-1,k-1,t)$. Let us take a subspace $R \in \mathcal{G}_q(n,t)$. If $R \subseteq W_{n-1}$, then

$R \cap W_{n-1}$ is an t-dimensional subspace. So it is contained in at least one $(k-1)$-dimensional subspace $V \in \mathcal{S}$, from which it follows that R is covered by some $V' \in \mathcal{S}$. On the other hand, if $R \nsubseteq W_{n-1}$, then $R \cap W_{n-1}$ is an $(t-1)$-dimensional and we will consider two cases, i.e. whether $(0,\ldots,0,1) \in R$ or not. In the first case, where $(0,\ldots,0,1) \in R$, then we extend $R \cap W_{n-1}$ to a t-dimensional subspace, which is itself, in turn contained in at least one element V of $\mathcal{S}$. Extending this V with $(0,\ldots,0,1)$ to a k-dimensional subspace, gives an element which covers R complety. For the second case, where $(0,\ldots,0,1) \notin R$, then $\langle R,(0,\ldots,0,1)\rangle \cap W_{n_1}$ is a t-dimensional subspace T. This subspace T is by definition of $\mathcal{S}'$, covered by some $(k-1)$-dimensional subspace V in W_{n-1}. Extending subspace V with $(0,\ldots,0,1)$, gives us the element V' of $\mathcal{S}'$ which contains $\langle R,(0,\ldots,0,1)\rangle$. It follows that R is in this case too covered by at least one k-dimensional element of $\mathcal{S}'$. So $\mathcal{S}'$ is a q-covering design $\mathscr{C}_q(n,k,t)$, which proves the lemma.

□

Corollary 4.4.3. *For all nonnegative integers δ, it follows that*

$$\mathcal{C}_q(n+\delta,k+\delta,t) \leqslant \mathcal{C}_q(n,k,t).$$

Lemma 4.4.4.

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

Proof. By Lemma 4.4.1, we have

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

Let $\delta = 2k-n$. If $k \geqslant \frac{n}{2}$, then δ is a nonnegative integer. Therefore, we can use Corollary 4.4.3 and we get

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

On the other hand, we know from Theorem 4.1.6 that $\mathcal{C}_q(n,k,1) \geqslant \frac{q^n-1}{q^k-1}$. If $2k \geqslant n$, we can write $n = k+r$, with $0 \leqslant r \leqslant k$, so

$$\left\lceil \frac{q^n-1}{q^k-1} \right\rceil = \left\lceil \frac{q^n-q^{n-k}}{q^k-1} + \frac{q^{n-k}-1}{q^k-1} \right\rceil = \left\lceil q^{n-k} + \frac{q^r-1}{q^k-1} \right\rceil = q^{n-k}+1,$$

for all $k = \left\lceil \frac{n}{2} \right\rceil, \left\lceil \frac{n}{2} \right\rceil + 1, \ldots, n-1$. Therefore, it follows that $\mathcal{C}_q(n,k,1) \geqslant q^{n-k}+1$, which completes the proof of the lemma. □

The proof of Lemma 4.4.4 indicates how q-covering designs which achieve the q-covering number $\mathcal{C}_q(n,k,1) = q^{n-k}+1$ can be constructed. There are several known constructions of spreads (see e.g. in Subsection 4.2.1), so we can start with the construction of a spread $\mathscr{S}_q(2(n-k),n-k,1)$. Whenever $k \geqslant \frac{n}{2}$, applying the construction described in the proof of Lemma 4.4.2 iteratively $\delta = 2k-n$ times, gives such a q-covering design.

On the other hand, the method for $k < \frac{n}{2}$, is completely different. In particular, we will make use of the construction shown in the following lemma, based on the proof of Theorem 11 in [17].

Lemma 4.4.5. *Let r be the remainder obtained when n is divided by k, and define $m = k + r$. Then there exists a set $\mathcal{X}$ consisting of one m-dimensional subspace of $\mathbb{F}_q^n$ and $\frac{q^n - q^m}{q^k - 1}$ subspaces of $\mathbb{F}_q^n$ of dimension k, such that*

$$V \cap V' = \{0\} \qquad \text{for all distinct } V, V' \in \mathcal{X}. \tag{4.4.1}$$

Proof. We will represent the vectors in $\mathbb{F}_q^n$ as tuples (x, y) with $x \in \mathbb{F}_{q^{n-m}}$ and $y \in \mathbb{F}_{q^m}$. Let α be a primitive element of $\mathbb{F}_{q^{n-m}}$ and let β be a primitive element of $\mathbb{F}_{q^m}$. First, we define

$$W \coloneqq \left\langle (0, \beta^0), (0, \beta^1), \ldots, (0, \beta^{m-1}) \right\rangle.$$

Since $\beta^0, \beta^1, \beta^2, \ldots, \beta^{m-1}$ are linearly independent over $\mathbb{F}_q$, we see that $\dim W = m$. Let $t = \frac{q^{n-m}-1}{q^k-1}$, which is an integer because k divides $n-m$ by our choice of m. Next, define $\gamma = \alpha^t$ and note that the multiplicative order of γ in $\mathbb{F}_{q^{n-m}}$ is $q^k - 1$. Therefore, γ is a primitive element of $\mathbb{F}_{q^k}$, as a subfield of $\mathbb{F}_{q^{n-m}}$. This implies that $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ form a basis for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Now, for $i = 0, 1, \ldots, t-1$ and $j = 0, 1, \ldots, q^m - 2$, we define the t subspaces of $\mathbb{F}_q^n$

$$U_i \coloneqq \left\langle (\alpha^i, 0), (\alpha^i\gamma, 0), \ldots, (\alpha^i\gamma^{k-1}, 0) \right\rangle \tag{4.4.2}$$

and the $t(q^m - 1)$ subspaces of $\mathbb{F}_q^n$

$$V_{ij} \coloneqq \left\langle (\alpha^i, \beta^j), (\alpha^i\gamma, \beta^{j+1}), \ldots, (\alpha^i\gamma^{k-1}, \beta^{j+k-1}) \right\rangle. \tag{4.4.3}$$

Since $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ are linearly independent over $\mathbb{F}_q$, it follows that $\dim U_i = \dim V_{ij} = k$ for all i and j. Consider the set

$$\mathcal{X} \coloneqq \left(\bigcup_i U_i \right) \cup \left(\bigcup_{i,j} V_{ij} \right) \cup W.$$

The number of k-dimensional subspaces in $\mathcal{X}$ is

$$t + t(q^m - 1) = \frac{q^{n-m} - 1}{q^k - 1} + \frac{q^{n-m} - 1}{q^k - 1}(q^m - 1) = \frac{q^n - q^m}{q^k - 1}.$$

Furthermore, $\mathcal{X}$ has also one subspace of dimension m. So it remains to be proven that (4.4.1) holds. First, note that for any nonzero vector $(x, y) \in \mathbb{F}_q^n = \mathbb{F}_{q^{n-m}} \times \mathbb{F}_{q^m}$, we have

$$\begin{aligned} (x, y) \in W &\Rightarrow x = 0, y \neq 0, \\ (x, y) \in U_i &\Rightarrow x \neq 0, y = 0, \\ (x, y) \in V_{ij} &\Rightarrow x \neq 0, y \neq 0, \end{aligned}$$

since both $\alpha^i, \alpha^i\gamma, \ldots, \alpha^i\gamma^{k-1}$ and $\beta^j, \beta^{j+1}, \ldots, \beta^{j+k-1}$ are linearly independent over $\mathbb{F}_q$, for all i and j. This implies that,

$$W \cap U_i = W \cap V_{ij} = U_i \cap V_{ij} = \{0\} \qquad \text{for all } i, j.$$

Next, observe that the construction of the subspaces U_i is similar to the construction of the subspaces H_i in Subsection 4.2.1, where these H_i form a Steiner structure $\mathscr{S}_q(1, k, n)$.

So it follows that the t subspaces $U_0, U_1, \ldots, U_{t-1}$ form a k-spread in $\mathbb{F}_q^{n-m}$. Therefore, $U_{i_1} \cap U_{i_2} = \{0\}$ for all $i_1 \neq i_2$. The same arguments lead us to the fact that also $V_{i_1 j_1} \cap V_{i_2 j_2} = \{0\}$ for all j_1 and j_2, whenever $i_1 \neq i_2$. In order to complete the proof, it remains to be shown that $V_{ij_1} \cap V_{ij_2} = \{0\}$ for every fixed i and all $j_1 \neq j_2$. Assume to the contrary that (x, y) is a nonzero vector in both V_{ij_1} and V_{ij_2}, and consider the corresponding linear combinations of the basis vectors in (4.4.3), i.e.

$$\begin{aligned} x &= a_0\alpha^i + a_1\alpha^i\gamma + \cdots + a_{k-1}\alpha^i\gamma^{k-1} \\ &= b_0\alpha^i + b_1\alpha^i\gamma + \cdots + b_{k-1}\alpha^i\gamma^{k-1} \end{aligned} \tag{4.4.4}$$

and

$$\begin{aligned} y &= a_0\beta^{j_1} + a_1\beta^{j_1+1} + \cdots + a_{k-1}\beta^{j_1+k-1} \\ &= b_0\beta^{j_2} + b_1\beta^{j_2+1} + \cdots + b_{k-1}\beta^{j_2+k-1}. \end{aligned} \tag{4.4.5}$$

Since $1, \gamma, \gamma^2, \ldots, \gamma^{k-1}$ are linearly independent over $\mathbb{F}_q$, it follows from (4.4.4) that $a_\ell = b_\ell$ for all ℓ. Hence, we can rewrite (4.4.5) as

$$(\beta^{j_1} - \beta^{j_2})(a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{k-1}\beta^{k-1}) = 0.$$

But since $1, \beta, \beta^2, \ldots, \beta^{k-1}$ are linearly independent over $\mathbb{F}_q$, this implies that $\beta^{j_1} = \beta^{j_2}$. Since β is a primitive root, it follows that $j_1 = j_2$, which is a contradiction. This completes the constructive proof of this lemma. □

Remark 4.4.6. If you take a one-dimensional subspace U of $\mathbb{F}_q^n$, then it follows from (4.4.1) that there is at most one subspace V of $\mathcal{X}$ that contains U. The total number of one-dimensional subspaces contained in some element of $\mathcal{X}$ is given by

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

which is exactly the total number of one-dimensional subspaces in $\mathbb{F}_q^n$. This means that every one-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one subspace of $\mathcal{X}$. This implies that $\mathcal{X}$ can be seen as a generalization of the notion of a spread to the case where k does not divide n. We will discuss this in the last chapter, were the construction of Lemma 4.4.5, used in Theorem 5.1.2, will give rise to the concept of partial spreads. Also note that if k divides n, the parameter m in Lemma 4.4.5 is just k, the construction is in fact the construction of a regular Desarguesian spread (see Subsection 4.2.1) and so, the set $\mathcal{X}$ is a spread.

Theorem 4.4.7.

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

Proof. As in Lemma 4.4.5, define r as the remainder obtained when n is divided by k, and let $m = k + r$. If $r = 0$, the theorem follows from Lemma 4.4.1. Assume now that k does not divide n and therefore $k < m < 2k$. In this case, we will use Lemma 4.4.5 and modify the set $\mathcal{X}$ to obtain a q-covering design $\mathscr{C}_q(n, k, 1)$ as follows. Let W denote the single m-dimensional subspace of $\mathcal{X}$ and let $\mathcal{S}$ be a q-covering design consisting of k-dimensional subspaces of W such that every one-dimensional subspace of W is contained

in at least one element of $\mathcal{S}$. Then clearly $\mathcal{S} \cup (\mathcal{X} \backslash \{W\})$ is a q-covering design $\mathscr{C}_q(n,k,1)$. Since $\dim W = m$, it follows that

$$\mathcal{C}_q(n,k,1) \leqslant \frac{q^n - q^m}{q^k - 1} + \mathcal{C}_q(m,k,1) = \frac{q^n - q^m}{q^k - 1} + q^{m-k} + 1 = \frac{q^n - q^r}{q^k - 1} + 1, \tag{4.4.6}$$

where the first equality follows from Lemma 4.4.4, since $k < m < 2k$. Note that k divides $n - r$, so $\frac{q^n - q^r}{q^k - 1}$ is an integer. Furthermore, since $r \neq 0$,

$$\left\lceil \frac{q^n - 1}{q^k - 1} \right\rceil = \left\lceil \frac{q^n - q^r}{q^k - 1} + \frac{q^r - 1}{q^k - 1} \right\rceil = \frac{q^n - q^r}{q^k - 1} + 1,$$

which is just the right hand side of (4.4.6). The other inequality, i.e.

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

follows from Theorem 4.1.6. □

Since q-covering designs and q-Turán designs are dual concepts, Corollary 4.1.5 gives us that $\mathcal{T}_q(n, n-1, t) = \mathcal{C}_q(n, n-t, 1)$. Together with the previous theorem, this implies the next corollary.

Corollary 4.4.8.

$$\mathcal{T}_q(n, n-1, t) = \left\lceil \frac{q^n - 1}{q^{n-t} - 1} \right\rceil.$$

In what follows we will also make use of the duality between q-covering designs and q-Turán designs. The q-covering number $\mathcal{C}_q(n, n-1, r)$ in particular will be achieved by examining the q-Turán numbers $\mathcal{T}_q(n,k,1)$. We begin with an elementary upper bound on $\mathscr{T}_q(n,k,t)$ that holds for all q, n, k and t, of which the proof enables us to construct a q-Turán design.

Lemma 4.4.9.

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

Proof. Consider a fixed subspace U of $\mathbb{F}_q^n$ of dimension $n - k + t$. Let $\mathcal{S}$ be the set of all t-dimensional subspaces of U. Then

$$|\mathcal{S}| = \begin{bmatrix} n-k+t \\ t \end{bmatrix}.$$

In order to find the inequality of the lemma, we will prove that this set $\mathcal{S}$ is a q-Turán design $\mathscr{T}_q(n,k,t)$. So, take any arbitrary k-dimensional subspace V of $\mathbb{F}_q^n$. Then the intersection $U \cap V$ is a subspace of U of which the dimension is

$$\dim(U \cap V) = \dim U + \dim V - \dim(U + V) \geqslant (n - k + t) + k - n = t,$$

since $U + V$ cannot have a dimension larger than the dimension of the ambient space $\mathbb{F}_q^n$. This means that $U \cap V$ must contain at least one element of $\mathcal{S}$, so $\mathcal{S}$ is indeed a q-Turán design $\mathscr{T}_q(n,k,t)$, from which the lemma follows. □

Corollary 4.4.10.

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

Proof. From Corollary 4.1.5 we know that $\mathcal{C}_q(n,k,t) = \mathcal{T}_q(n,n-t,n-k)$. We use Lemma 4.4.9 to obtain an upper bound on $\mathcal{T}_q(n,n-t,n-k)$. Observing that

$$\begin{bmatrix} n-(n-t)+(n-k) \\ n-k \end{bmatrix} = \begin{bmatrix} n-k+t \\ (n-k+t)-(n-k) \end{bmatrix} = \begin{bmatrix} n-k+t \\ t \end{bmatrix}$$

gives us the requested upper bound on $\mathcal{C}_q(n,k,t)$. □

Theorem 4.4.11.

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

Proof. Applying Lemma 4.4.9 for the case with $t = 1$, gives us

$$\mathcal{T}_q(n,k,1) \leqslant \frac{q^{n-k+1}-1}{q-1}. \tag{4.4.7}$$

Hence, it remains to be proven that $\frac{q^{n-k+1}-1}{q-1}$ is also a lower bound on $\mathcal{T}_q(n,k,1)$. Assume to the contrary that $\mathcal{S}$ is an arbitrary set of one-dimensional subspaces with $|\mathcal{S}| = \frac{q^{n-k+1}-1}{q-1} - 1$. We claim that this set $\mathcal{S}$ cannot be a q-Turán design $\mathscr{T}_q(n,k,1)$. This means that there has to be at least one k-dimensional subspace of $\mathbb{F}_q^n$ that does not contain any element of $\mathcal{S}$. Define U as the largest subspace of $\mathbb{F}_q^n$ such that $U \cap V = \{0\}$ for all $V \in \mathcal{S}$ and let $m = \dim U$. Note that $m \geqslant 0$, since $U = \{0\}$ satisfies this condition. If $m \geqslant k$, then every k-dimensional subspace of U does not contain any element of $\mathcal{S}$, which proves the theorem. Thus, let us assume that $m < k$. Now take a fixed one-dimensional subspace $V \in \mathcal{S}$ and consider the vector space $\langle V \cup U \rangle$, spanned by all the vectors in the set $V \cup U$. Since $\dim U = m$, $\dim V = 1$ and $U \cap V = \{0\}$, it follows that $\dim \langle V \cup U \rangle = m+1$. Thus $\langle V \cup U \rangle$ contains exactly $q^{m+1} - q^m$ vectors that are not contained in U. Hence

$$\begin{aligned} \left| \bigcup_{V \in \mathcal{S}} \langle V \cup U \rangle \right| &\leqslant |\mathcal{S}| \cdot (q^{m+1} - q^m) + |U| \\ &= \left(\frac{q^{n-k+1}-1}{q-1} - 1\right) \cdot q^m(q-1) + q^m = q^{n-k+m+1} - q^m(q-1). \end{aligned} \tag{4.4.8}$$

Because we assumed that $m < k$, $q^{n-k+m+1} \leqslant q^n$ and so the right hand side of (4.4.8) is bounded by $q^n - 1$. Therefore, there exists a nonzero vector $x \in \mathbb{F}_q^n$ such that $x \notin \cup_{V \in \mathcal{S}} \langle V \cup U \rangle$. Consider the vector space $W := \langle \{x\} \cup U \rangle$. Suppose that for an arbitrary $V \in \mathcal{S}$, there exists a vector $y \neq 0$ such that $y \in W \cap V$. Since $y \notin U \cap V$, it follows that $y \notin U$ and so y has to be contained in $\{x\} \cup U$. But $y \cup U = \{x\} \cup U \subseteq \langle V \cup U \rangle$ gives a contradiction, so we have $W \cap V = \{0\}$ for all $V \in \mathcal{S}$ and $\dim W = m+1$. But this contradicts the maximality of U. This implies that we must have $m \geqslant k$, which

proves the claim that any set $\mathcal{S}$ of one-dimensional subspaces with $|\mathcal{S}| < \frac{q^{n-k+1}-1}{q-1}$ cannot be a q-Turán design $\mathscr{T}_q(n,k,1)$, so

$$|\mathscr{T}_q(n,k,1)| \geqslant \frac{q^{n-k+1}-1}{q-1},$$

which gives us, together with the inequality (4.4.7), the exact value of the q-Turán number $\mathcal{T}_q(n,k,1)$. □

This theorem, together with the fact that $\mathcal{T}_q(n,n-t,1) = \mathcal{C}_q(n,n-1,t)$, leads us to the next corollary.

Corollary 4.4.12.

$$\mathcal{C}_q(n,n-1,t) = \frac{q^{t+1}-1}{q-1}.$$

The duality between designs $\mathscr{T}_q(n,n-t,1)$ and $\mathscr{C}_q(n,n-1,t)$ also helps to construct q-covering designs which achieve the q-covering number $\mathcal{C}_q(n,n-1,t)$ (see Corollary 4.4.12). First construct a q-Turán design $\mathscr{T}_q(n,n-t,1)$ as in Lemma 4.4.9, i.e. construct a set $\mathcal{S}$ of all one-dimensional subspaces of a fixed vector space U in $\mathbb{F}_q^n$ of dimension $t+1$. Then take the orthogonal complement of $\mathcal{S}$ as in Theorem 4.1.4 and so $\mathcal{S}^\perp = \{V^\perp \in \mathcal{G}_q(n,n-1) | V \in \mathcal{S}\}$ is a q-covering design with $|\mathcal{S}^\perp| = \frac{q^{t+1}-1}{q-1}$.

4.4.2 An upper bound on q-covering numbers

In the previous section we determined the q-covering numbers $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,t)$ and the corresponding q-Turán numbers $\mathcal{T}_q(n,n-1,t)$ and $\mathcal{T}_q(n,k,1)$. We also examined some general upper bounds on q-covering numbers and q-Turán numbers in Corollary 4.4.10 and Lemma 4.4.9 respectively. Although in [18], Etzion and Vardy make the remark that these bounds are tight for $t=1$ (see Theorem 4.4.11 and Corollary 4.4.12), these bounds are quite weak for $t \geqslant 2$. Therefore they introduce a recursive construction of q-covering designs that leads to a new general upper bound on $\mathcal{C}_q(n,k,t)$, which improves Corollary 4.4.10 considerably.

Theorem 4.4.13.

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

Proof. As in Lemma 4.4.2, we represent the ambient n-dimensional vector space as

$$\mathbb{F}_q^n = W_{n-1} \times \mathbb{F}_q = \left\{(x,\alpha) | x \in \mathbb{F}_q^{n-1}, \alpha \in \mathbb{F}_q\right\},$$

for some $W_{n-1} \in \mathcal{G}_q(n,n-1)$. Let $\mathcal{S}_1$ be a q-covering design $\mathscr{C}_q(n-1,k,t)$ in W_{n-1} of size $\mathcal{C}_q(n-1,k,t)$ and $\mathcal{S}_2$ a q-covering design $\mathscr{C}_q(n-1,k-1,t)$ in W_{n-1} of size $\mathcal{C}_q(n-1,k-1,t)$. Given a subspace V of W_{n-1}, we want to lift this up to the n-dimensional vector space $\mathbb{F}_q^n$ by defining the corresponding subspace in $\mathbb{F}_q^n$ as

$$V \times \{0\} = \{(v,0) \in \mathbb{F}_q^n \,|\, v \in V\}.$$

It also follows that $\dim(V \times \{0\}) = \dim V$. This construction will be used to lift up $\mathcal{S}_1$, i.e.

$$\mathcal{S}_1' \coloneqq \{V \times \{0\} \subset \mathbb{F}_q^n \,|\, V \in \mathcal{S}_1\}.$$

Furthermore, for any $V \in \mathcal{S}_2$, there are exactly $q^{n-1-(k-1)} = q^{n-k}$ cosets of V in W_{n-1}. This implies that there are q^{n-k} distinct subspaces of the form $(V \times \{0\}) \oplus \langle (x,1) \rangle$, for a fixed $V \in \mathcal{S}_2$. Let us now define

$$\mathcal{S}_2' \coloneqq \left\{ (V \times \{0\}) \oplus \langle (x,1) \rangle \subset \mathbb{F}_q^n \,|\, V \in \mathcal{S}_2, x \in W_{n-1} \right\},$$

and $\mathcal{S}' = \mathcal{S}_1' \cup \mathcal{S}_2'$. By construction, this set $\mathcal{S}'$ consists of subspaces of $\mathbb{F}_q^n$, each of dimension k, and the number of elements of $\mathcal{S}'$ is

$$|\mathcal{S}'| = |\mathcal{S}_1| + q^{n-k}|\mathcal{S}_2| = \mathcal{C}_q(n-1,k,t) + q^{n-k}\mathcal{C}_q(n-1,k-1,t-1). \tag{4.4.9}$$

Consequently, if we can show that $\mathcal{S}'$ is a q-covering design $\mathscr{C}_q(n,k,t)$, the q-covering number $\mathcal{C}_q(n,k,r)$ is bounded by (4.4.9). So it remains to be shown that for each t-dimensional subspace U of $\mathbb{F}_q^n$ there is a subspace $V' \in \mathcal{S}'$ such that $U \subset V'$.

First, if the subspace $U \subset W_{n-1} \times \{0\}$, then U is contained in at least one subspace of $\mathcal{S}_1'$, since $\mathcal{S}_1'$ is a q-covering design $\mathscr{C}_q(n-1,k,t)$ in $W_{n-1} \times \{0\}$. If U is not a subset of $W_{n-1} \times \{0\}$, it must contain a vector of the form $(x,1)$ for some $x \in W_{n-1}$. This implies that U can be spanned by vectors of the form $\{(u_1,0),(u_2,0),\ldots,(u_{t-1},0),(x,1)\}$ and can be represented as $(U' \times \{0\}) \oplus \langle (x,1) \rangle$ with $U' = \langle u_1, u_2, \ldots, u_{t-1} \rangle$. Since U' is a $(t-1)$-dimensional subspace of W_{n-1} and $\mathcal{S}_2$ is a q-covering design $\mathscr{S}_q(n-1,k-1,t-1)$ in W_{n-1}, there exists a subspace $V \in W_{n-1}$ which covers the subspace U'. This means that the corresponding subspace $(V \times \{0\}) \oplus \langle (x,1) \rangle$ of $\mathcal{S}_2'$ contains U. □

The construction of the previous theorem can be iterated to obtain an upper bound on the minimum size of a q-covering design $\mathscr{C}_q(n,k,t)$ for any given set of parameters. For example, we use Theorem 4.4.13 to derive an upper bound on $\mathcal{C}_2(5,3,2)$. Since from Corollary 4.4.12 we know that $\mathcal{C}_2(4,3,2) = 7$ and from Theorem 4.4.7 it follows that $\mathcal{C}_2(4,2,1) = 5$ and so

$$\mathcal{C}_2(5,3,2) \leqslant 2^2\mathcal{C}_2(4,2,1) + \mathcal{C}_2(4,3,2) = 2^2 \cdot 5 + 7 = 27. \tag{4.4.10}$$

This bound[3] implies other upper bounds, i.e.

$$\begin{aligned} \mathcal{C}_2(6,3,2) &\leqslant 2^3\mathcal{C}_2(5,2,1) + \mathcal{C}_2(5,3,2) \leqslant 2^3 \cdot 11 + 27 = 115, \\ \mathcal{C}_2(7,3,2) &\leqslant 2^4\mathcal{C}_2(6,2,1) + \mathcal{C}_2(6,3,2) \leqslant 2^4 \cdot 21 + 115 = 451, \end{aligned}$$

since we can use Theorem 4.4.7 again for the q-covering numbers $\mathcal{C}_q(n,k,t)$ with $t = 1$. This example shows how to obtain an explicit upper bound for the parameter $t = 2$. Indeed, we have

$$\begin{aligned} \mathcal{C}_q(n,k,2) &\leqslant q^{n-k}\mathcal{C}_q(n-1,k-1,1) + \mathcal{C}_q(n-1,k,2) \\ &\leqslant q^{n-k}\mathcal{C}_q(n-1,k-1,1) + q^{n-1-k}\mathcal{C}_q(n-2,k-1,1) + \mathcal{C}_q(n-2,k,2). \end{aligned}$$

[3] In [18] it is shown that $\mathcal{C}_2(5,3,2)$ is exactly 27.

Continuing in this manner, every q-covering number in the upper bound can be calculated with Theorem 4.4.7, except for the last one. Corollary 4.4.12 gives the solution, i.e. the process can be stopped if we reach $\mathcal{C}_q(n-(n-k-1),k,2) = \frac{q^3-1}{q-1}$. This means, we arrive at the following upper bound:

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

4.4.3 Schönheim bound

In search of the exact values of q-covering numbers, we want to find q-covering designs with a size as small as possible. So it is not strange that one wants to bring down these values with upper bounds. However, it is also useful to have a notion of some lower bounds to bring down the interval of possible values of $C_q(n,k,t)$. We already have the elementary lower bound of Theorem 4.1.6. In this subsection, we present a lower bound, which is the q-analogue of the bound of Schönheim for classical coverign designs.

We will proof this bound and its corollary, based on the proof in [18], with the same techniques as the proof of Theorem 1.2.7 and Corollary 1.2.8.

Theorem 4.4.14 (Schönheim bound)**.**

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

Proof. Consider $\mathcal{S}$, a q-covering design $\mathscr{C}_q(n,k,t)$ with $|\mathcal{S}| = \mathcal{C}_q(n,k,t)$. Each element of $\mathcal{S}$ contains $\begin{bmatrix} k \\ 1 \end{bmatrix} = \frac{q^k-1}{q-1}$ one-dimensional subspaces of $\mathbb{F}_q^n$ and the total number of such subspaces is $\frac{q^n-1}{q-1}$. So the average number of elements of $\mathcal{S}$ in which a one-dimensional subspace is contained, is $\frac{q^k-1}{q^n-1}|\mathcal{S}|$. So there has to be a one-dimensional subspace $W_1 \subset \mathbb{F}_q^n$ that is contained in at most $\frac{q^k-1}{q^n-1}|\mathcal{S}|$ elements of $\mathcal{S}$. Now we will use a technique similar to that of Theorem 4.2.1. We can represent $\mathbb{F}_q^n$ as $W_1 \oplus W_{n-1}$, where W_{n-1} is an $(n-1)$-dimensional subspace. Let us now define a set

$$\mathcal{S}' \coloneqq \{U \cap W_{n-1} | U \in \mathcal{S} \text{ and } W_1 \subset U\} .$$

This construction implies that

$$|\mathcal{S}'| \leqslant \frac{q^k-1}{q^n-1}|\mathcal{S}| = \frac{q^k-1}{q^n-1}\mathcal{C}_q(n,k,t).$$

To prove the theorem, we will show that $\mathcal{S}'$ is a q-covering design $\mathscr{C}_q(n-1,k-1,t-1)$ of W_{n-1}. Since W_{n-1} and W_1 are disjoint and $W_1 \subset U$ for every $U \in \mathcal{S}$ corresponding to an element of $\mathcal{S}'$, it follows that $\mathcal{S}'$ consists of $(k-1)$-dimensional subspaces of W_{n-1}. Now take an arbitrary $(t-1)$-dimensional subspace V of W_{n-1}. Then $W_1 \oplus V$ is a t-dimensional subspace of $\mathbb{F}_q^n$ and therefore, there exists a $U \in \mathcal{S}$ such that $W_1 \oplus V \subset U$. Consequently, $U' = U \cap W_{n-1}$ is an element of $\mathcal{S}'$ and $V \subset U'$. This proves that $\mathcal{S}'$ is a q-covering design $\mathscr{C}_q(n-1,k-1,t-1)$ of W_{n-1} and the theorem follows. □

Corollary 4.4.15.

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

Proof. Applying Theorem 4.4.14 iteratively $t-1$ times and observing that, by Theorem 4.4.7,

$$\mathcal{C}_q(n-t+1,k-t+1,1) = \left\lceil \frac{q^{n-t+1}-1}{q^{k-t+1}-1} \right\rceil ,$$

the theorem follows. □

Chapter 5

Partial spreads and partial spread codes in random network coding

5.1 Spread codes and partial spread codes

In the Section 1.2, we already mentioned that there is a nice link between design theory and coding theory. For instance in Example 1.2.11, codes in the Johnson space can be constructed from Steiner systems.

We can do an analogous construction to obtain an (n, M, d, k)-code in $\mathcal{G}_q(n,k)$ from a Steiner structure $\mathscr{S}_q(t,k,n)$. We recall that a Steiner structure $\mathscr{S}_q(t,k,n)$ is also called a $(t,k)-$spread, and that this is a subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,t)$ is contained in exactly one subspace of $\mathcal{S}$. This means that the intersection of two elements $U, V \in \mathcal{S}$ cannot contain a t-dimensional subspace. Hence, $\dim(U \cap V) \leqslant t-1$ and

$$d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V) \geqslant 2(k-t+1).$$

Furthermore, if we can find two elements of $\mathcal{S}$ with an intersection of dimension $t-1$, it follows that the code obtained by taking the elements of the Steiner structure $\mathscr{S}_q(t,k,n)$, has minimum distance $2(k-t+1)$. Fix a $(t-1)$-dimensional subspace X and count the pairs (U,T) where U is a k-dimensional block of $\mathcal{S}$ containing X, T an element of $\mathcal{G}_q(t,n)$ containing X and such that T is a subspace of U. This implies that the number of elements of $\mathcal{S}$ through a fixed $(t-1)$-dimensional subspace is $\frac{\begin{bmatrix} n-t+1 \\ 1 \end{bmatrix}}{\begin{bmatrix} k-t+1 \\ 1 \end{bmatrix}} \geqslant 2$. Consequently, if you take the elements of a Steiner structure $\mathscr{S}_q(t,k,n)$ as codewords, this is an (n, M, d, k)-code in $\mathcal{G}_q(n,k)$ with $M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}$ and $d = 2(k-t+1)$.

Remark 5.1.1. Note that we already mentioned in Remark 3.1.17 that any $(n, M, 2\delta, k)$-code with $M = \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}}$ is a Steiner structure $\mathscr{S}_q(k-\delta+1, k, n)$.

In this chapter we are interested in the special case of Steiner structures with parameter $t = 1$, i.e. spreads. If we want to emphasize that the subspaces of the spread are of dimension k, sometimes the concept k-spread is used (see e.g. [21]). In other words, a

k-spread of $\mathbb{F}_q^n$ is a partition of $\mathbb{F}_q^n$ in k-dimensional subspaces. The associated network codes are called ***spread codes***. Since a spread $\mathscr{S}_q(1,k,n)$ leads to an $(n,M,2k,k)$-code, we can translate the bounds for q-covering designs and Steiner structures to bounds for specific codes. In particular, Lemma 4.4.1 implies that

$$\mathcal{A}_q(n,2k,k) = \frac{q^n-1}{q^k-1}, \qquad \text{whenever } k|n.$$

This result can be extended for the case where k does not divide n. We will use the construction from Etzion and Vardy ([17]), shown in the proof of Lemma 4.4.5, to prove the following theorem.

Theorem 5.1.2. *Let $n \equiv r \pmod{k}$. Then for all q, we have*

$$\mathcal{A}_q(n,2k,k) \geqslant \frac{q^n - q^k(q^r-1)-1}{q^k-1}.$$

Proof. Let r be the remainder obtained when k is divided into n, and define $m = k+r$. By Lemma 4.4.5, we get a set $\mathcal{X}$ consisting of one m-dimensional subspace W of $\mathbb{F}_q^n$ and $\frac{q^n-q^m}{q^k-1}$ subspaces of $\mathbb{F}_q^n$ of dimension k, such that $U \cap V = \{0\}$ for all $U,V \in \mathcal{X}$. Define $\mathcal{C}$ to be the set of all k-dimensional subspaces of $\mathcal{X}$ together with an arbitrary k-dimensional subspace of W[1]. It follows that $U \cap V = \{0\}$ for every element $U,V \in \mathcal{C}$, which means that the minimum distance of $\mathcal{C}$ is $2k$. Furthermore the size of this code $\mathcal{C}$ is

$$\frac{q^n-q^m}{q^k-1} + 1 = \frac{q^n+q^k-q^m-1}{q^k-1},$$

which gives us the lower bound of this theorem. □

The code constructed in the above theorem is a generalisation of a spread code, which we will define as a partial spread code.

Definition 5.1.3. A ***partial k-spread*** of $\mathbb{F}_q^n$ is a subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ such that $U \cap V = \{0\}$ for any $U,V \in \mathcal{S}$ with $U \neq V$. A partial k-spread of $\mathbb{F}_q^n$ is a q-ary network code of length n, dimension k and minimum distance $2k$. We will call such a code a ***partial spread code***. If a partial k-spread cannot be extended to a larger partial k-spread, we call it a ***maximal*** partial k-spread.

This structure will be the topic of this last chapter. Section 5.2 is based on the paper of Eisfeld and Storme ([14]) and Section 5.3 on the recent article of Gorla and Ravagnani ([21]).

From Theorem 5.1.2 we have a lower bound for partial spreads. In the following theorem, an upper bound is given.

[1] In the proof of Theorem 11 in [17], the subspace W is defined as the k-dimensional vector space $\langle (0,\beta^0),(0,\beta^1),\ldots,(0,\beta^{k-1})\rangle$ instead of $W := \langle (0,\beta^0),(0,\beta^1),\ldots,(0,\beta^{m-1})\rangle$ in the proof of Lemma 4.4.5.

Theorem 5.1.4. *Let $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ be a partial spread code. Denote by r the remainder obtained dividing n by k. Then*

$$|\mathcal{C}| \leqslant \frac{q^n - q^r}{q^k - 1}.$$

Proof. From the definition of a partial spread code, we know that $\mathcal{C}$ is a set of subspaces of dimension k with trivial pairwise intersections. This property implies that $|\mathcal{C}| \cdot (q^k - 1) + 1 \leqslant q^n$. Since k divides $n - r$, $\frac{q^{n-r}-1}{q^k-1}$ is an integer, so it follows that

$$|\mathcal{C}| \leqslant \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor = \left\lfloor \frac{q^r(q^{n-r} - 1)}{q^k - 1} + \frac{q^r - 1}{q^k - 1} \right\rfloor = \frac{q^n - q^r}{q^k - 1}. \qquad \square$$

5.2 (Partial) t-spreads in finite projective spaces

In the next section we describe the work of Gorla and Ravagnani ([21]), in which they constructed a special partial spread code whose size attains the lower bound of Theorem 5.1.2. This construction can be related to the construction of partial spreads in projective space, which we will examine in this section, based on [14].

Note that in this section we consider (partial) t-spreads in $\mathrm{PG}(d,q)$. Because of the link between vector spaces and projective spaces, the relation of the parameters of the different sections is $k = t + 1$ and $n = d + 1$. A ***t-spread*** is a set $\mathcal{S}$ of t-dimensional subspaces of $\mathcal{P} = \mathrm{PG}(d,q)$ which partitions $\mathcal{P}$, i.e. every point of $\mathcal{P}$ is contained in exactly one element of $\mathcal{S}$. As observed in Subsection 4.2.1, a t-spread can only exist if the number of points of a t-dimensional subspace divides the number of points of the whole space. This means that $\frac{q^{t+1}-1}{q-1}$ has to be a divisor of $\frac{q^{d+1}-1}{q-1}$ and hence $\frac{q^{d+1}-1}{q^{t+1}-1}$ has to be an integer, which holds if and only if $(t+1)|(d+1)$. This necessary condition is also sufficient, since we can construct a t-spread, whenever $t+1$ divides $d+1$. The construction we present below, is in fact the same as the construction in Subsection 4.2.1.

An element of a t-spread can be seen as a projective space $\mathrm{PG}(t,q)$ or as a vector space $V(t+1,q)$. Furthermore, we have the congruence $\mathbb{F}_{q^{t+1}} \cong V(t+1,q)$, where the addition is just as in $\mathbb{F}_{q^{t+1}}$, but the only permitted multiplication is the multiplication with scalars of $\mathbb{F}_q$. We also have that $\mathcal{P} = \mathrm{PG}(d,q) = V(d+1,q) \cong \mathbb{F}_{q^{d+1}}$. Since $t+1$ divides $d+1$, it follows that $\mathbb{F}_{q^{t+1}} \subseteq \mathbb{F}_{q^{d+1}}$. This implies that the field $\mathbb{F}_{q^{t+1}}$ is a $(t+1)$-dimensional subspace of $V(d+1,q)$ and hence a t-dimensional projective subspace of $\mathcal{P}$. The same holds for all cosets $\omega \cdot \mathbb{F}_{q^{t+1}}$, with $\omega \in \mathbb{F}_{q^{d+1}} \backslash \{0\}$. The sets $\omega \cdot \mathbb{F}_{q^{t+1}} \backslash \{0\}$ form a partition of $\mathbb{F}_{q^{d+1}} \backslash \{0\}$, which leads to a t-spread of $\mathcal{P}$.

This gives us the following equivalent result of Corollary 4.2.3.

Theorem 5.2.1. *In $\mathrm{PG}(d,q)$, a t-spread exists if and only if $t+1$ divides $d+1$.*

Consequently, if $t+1$ does not divide $d+1$, a t-spread of $\mathcal{P} = \mathrm{PG}(d,q)$ does not exist. Nevertheless, we can generalize this concept by examining sets of pairwise disjoint t-dimensional subspaces of $\mathcal{P}$, i.e. ***partial t-spreads***. In particular, the question arises which are the largest partial t-spreads of $\mathcal{P}$. In Theorem 5.1.4 we already showed an upper bound on the number of elements of a partial spread code. This corresponds to the following theorem in the case of projective spaces.

Theorem 5.2.2. *Let $d = h(t+1)+r-1$, where $1 \leqslant r \leqslant t$, and let $\mathcal{P} = \mathrm{PG}(d,q)$. A partial t-spread $\mathcal{S}$ of $\mathcal{P}$ contains at most $q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1}$ elements.*

Proof. The number of points of $\mathcal{P}$ is $\frac{q^{h(t+1)+r}-1}{q-1} = q^r \frac{q^{h(t+1)}-1}{q-1} + \frac{q^r-1}{q-1}$, where the first term is a multiple of $\frac{q^{t+1}-1}{q-1}$, i.e. the number of points of a t-dimensional subspace. This gives us the upper bound of the theorem. □

In what follows we want to see how close we can come to the bound of Theorem 5.2.2. Therefore, we will give an example of a partial t-spread, due to Beutelspacher ([3]).

Lemma 5.2.3. *Let U be an s-dimensional subspace of $\mathcal{P} = \mathrm{PG}(s+t+1,q)$, where $s \geqslant t$. Then there exists a set $\mathcal{S}$ of t-dimensional subspaces of $\mathcal{P}$ which do not intersect U such that every point of $\mathcal{P}\backslash U$ is contained in exactly one element of $\mathcal{S}$.*

Proof. Consider the projective space $\mathcal{P}' = \mathrm{PG}(2s+1,q)$ containing $\mathcal{P}$. Since $s+1$ divides $2s+1+1$, we can construct an s-spread $\mathcal{S}'$ of $\mathcal{P}'$ which contains U (see e.g. the construction in the beginning of this section where U is the t-dimensional subspace of $\mathcal{P}$ associated with the field $\mathbb{F}_{q^{t+1}}$ of which we take all the cosets). For every element V of $\mathcal{S}'\backslash\{U\}$, it follows that $V + \mathcal{P} \subseteq \mathcal{P}'$, so we have

$$\dim(V \cap \mathcal{P}) = \dim(V) + \dim(\mathcal{P}) - \dim(V+\mathcal{P}) \geqslant s+s+t+1-(2s+1) = t.$$

Since U is disjoint to every element $V \in \mathcal{S}'\backslash\{U\}$, the intersection cannot be larger. This means that each element of $\mathcal{S}'\backslash\{U\}$ intersects $\mathcal{P}$ exactly in a t-dimensional subspace. The set of these intersections is the set $\mathcal{S}$ we are looking for. □

Theorem 5.2.4. *Let U be an $(r+t)$-dimensional subspace of $\mathcal{P} = \mathrm{PG}(h(t+1)+r-1,q)$, where $1 \leqslant r \leqslant t$ and $h > 1$. Then there is a set $\mathcal{S}$ of t-dimensional subspaces of $\mathcal{P}$ which do not intersect U, such that every point of $\mathcal{P}\backslash U$ is contained in exactly one element of $\mathcal{S}$.*

Proof. Applying Lemma 5.2.3 for $s = t+r, 2(t+1)+r-1, \ldots, (h-1)(t+1)+r-1$, gives us a set $\mathcal{S}$ of t-dimensional subspaces of $\mathcal{P}$, which are mutually disjoint and for which every point of $\mathcal{P}\backslash U$ is covered by exactly one element of $\mathcal{S}$. □

Corollary 5.2.5. *Let $t, h \geqslant 1$ and $1 \leqslant r \leqslant t$. In $\mathcal{P} = \mathrm{PG}(h(t+1)+r-1,q)$ there exists a partial t-spread $\mathcal{S}$ with $|\mathcal{S}| = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - q^r + 1$.*

Proof. Take the set $\mathcal{S}'$ of t-dimensional subspaces of $\mathcal{P}$ as in Theorem 5.2.4. The number of points covered by this set is $\frac{q^{h(t+1)+r}-1}{q-1} - \frac{q^{t+r+1}-1}{q-1} = \frac{q^{h(t+1)+r}-q^{t+r+1}}{q-1}$. Dividing this by the number of points of a t-dimensional subspace, i.e. $\frac{q^{t+1}-1}{q-1}$, gives us

$$\frac{q^{h(t+1)+r}-q^{t+r+1}}{q^{t+1}-1} = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - q^r.$$

Adding one t-dimensional subspace of U to $\mathcal{S}'$, gives us a partial spread $\mathcal{S}$ of size $|\mathcal{S}| = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - q^r + 1$. □

The construction of Beutelspacher, explained above, is visualized in the following figure. You can see this as a 'partition in slices'. This technique is the basis of the construction of the partial spread code $\mathscr{C}_q(k, n; p, p')$ in Theorem 5.3.4.

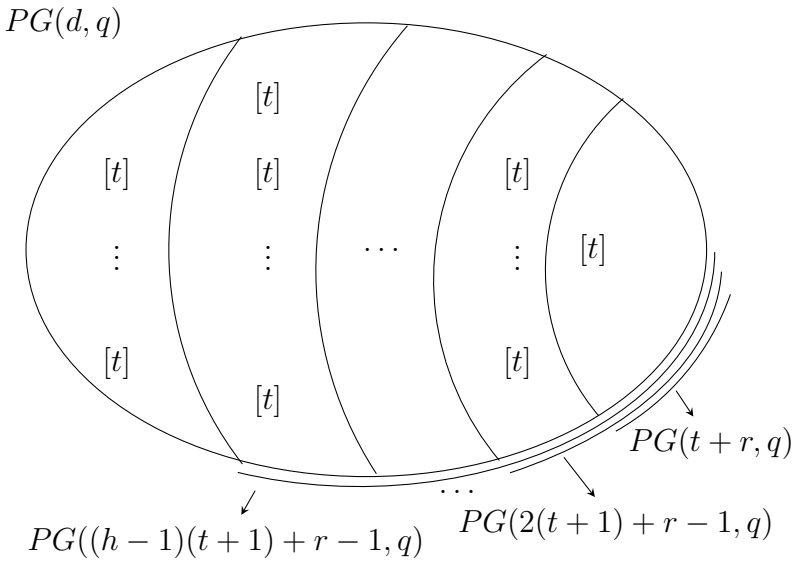


Figure 5.1: Visualisation of the construction from Corollary 5.2.5 of a partial spread

To end this section, we will prove[2] an upper bound on the size of a partial t-spread of $\mathrm{PG}(d, q)$. First we say something about the holes. A point $P \in \mathcal{P}$ is a ***hole*** of the partial t-spread $\mathcal{S}$ if it is not contained in an element of $\mathcal{S}$.

Lemma 5.2.6. *Let $\mathcal{S}$ be a partial t-spread in $\mathcal{P} = \mathrm{PG}(d, q)$, where $d = h(t+1) - 1 + r$, $1 \leqslant r \leqslant t$. Let $|\mathcal{S}| = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - s$. Then the number of holes is $\frac{q^r-1}{q-1} + s \cdot \frac{q^{t+1}-1}{q-1}$ and the number of holes in a hyperplane is congruent to $\frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} \pmod{q^t}$.*

Proof. Since a partial spread $\mathcal{S}$ consists of $|\mathcal{S}|$ pairwise disjoint t-dimensional subspaces and since the holes are the points of $\mathcal{P}$ not contained in $\mathcal{S}$, the number of holes is exactly

$$\begin{aligned} |\mathcal{P}| - |\mathcal{S}| \cdot \frac{q^{t+1}-1}{q-1} &= \frac{q^{h(t+1)+r}-1}{q-1} - q^r \cdot \frac{q^{h(t+1)}-1}{q-1} + s \cdot \frac{q^{t+1}-1}{q-1} \\ &= \frac{q^r-1}{q-1} + s \cdot \frac{q^{t+1}-1}{q-1}. \end{aligned}$$

To prove the second part, let H be a hyperplane of $\mathcal{P}$. Then an element V of $\mathcal{S}$ is contained in H or intersects H in a $(t-1)$-dimensional subspace. This means that V intersects H either in $\frac{q^{t+1}-1}{q-1} = \frac{q^t-1}{q-1} + q^t$ or in $\frac{q^t-1}{q-1}$ points, which is in any case $\frac{q^t-1}{q-1} \pmod{q^t}$ points. Since

$$|\mathcal{S}| = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - s = q^r \cdot (1 + q^t \cdot \frac{q^{h(t+1)-t}-q}{q^{t+1}-1}) - s,$$

[2] This approach is based on the proof of Theorem 2.7 in [14].

it follows that $|\mathcal{S}| \equiv q^r - s \pmod{q^t}$.

This implies that the number of points of H contained in an element of $\mathcal{S}$ is

$$\frac{q^t-1}{q-1} \cdot |\mathcal{S}| \equiv \frac{q^t-1}{q-1} \cdot (q^r - s) \pmod{q^t}.$$

Consequently, the number of holes in H is congruent to

$$\begin{aligned} |H| - \frac{q^t-1}{q-1} \cdot (q^r - s) &= \frac{q^{h(t+1)-1+r}-1}{q-1} - q^r \cdot \frac{q^t-1}{q-1} + s\frac{q^t-1}{q-1} \\ &= q^t \cdot \frac{q^{(h-1)(t+1)+r} - q^r}{q-1} + \frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} \\ &\equiv \frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} \pmod{q^t}. \end{aligned}$$

□

Theorem 5.2.7. *Let $\mathcal{S}$ be a partial t-spread in $\mathcal{P} = \mathrm{PG}(d,q)$, where $d = h(t+1)-1+r$, $1 \leqslant r \leqslant t$. Let $|\mathcal{S}| = q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - s$. Then*

(i) $s \geqslant q-1$,

(ii) $s > \frac{q^r-1}{2} - \frac{q^{2r-t-1}}{5}$.

Furthermore, there exists an example with $s = q^r - 1$.

Proof. (i) First, we want to prove that $s \geqslant q-1$.

Assume to the contrary that $s \leqslant q-2$. Therefore,

$$\frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} \leqslant \frac{q^r-1}{q-1} + (q-2) \cdot \frac{q^t-1}{q-1} = \frac{q^r-1}{q-1} + q^t - 1 - \frac{q^t-1}{q-1} < q^t,$$

and so, from Lemma 5.2.6, it follows that any hyperplane H contains at least $\frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1}$ holes. Double counting of the incident pairs (H,P), where H is a hyperplane of $\mathcal{P}$ and P a hole, gives us the inequality

$$\left(\frac{q^r-1}{q-1} + s \cdot \frac{q^{t+1}-1}{q-1}\right) \cdot \frac{q^d-1}{q-1} \geqslant \frac{q^{d+1}-1}{q-1} \cdot \left(\frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1}\right)$$

which is equivalent to

$$\begin{gathered} s\left[(q^{t+1}-1)(q^d-1) - (q^t-1)(q^{d+1}-1)\right] \geqslant (q^{d+1}-1)(q^r-1) - (q^d-1)(q^r-1) \\ \Leftrightarrow \\ s\left[q^d(q-1) - q^t(q-1)\right] \geqslant q^d(q-1)(q^r-1) \\ \Leftrightarrow \\ s(q^d - q^t) \geqslant q^d(q^r-1). \end{gathered}$$

Since we assumed that $s \leqslant q-2$, it follows that

$$\begin{aligned} q^{d+1} - 2q^d - (q-2)q^t = (q-2)(q^d - q^t) &\geqslant s(q^d - q^t) \\ &\geqslant q^d(q^r - 1) = q^{d+r} - q^d \\ &> q^{d+r} - 2q^d \\ &> q^{d+1} - 2q^d - (q-2)q^t, \end{aligned}$$

which gives a contradiction.

(ii) The proof of the second part will give us that $s > \frac{q^r-1}{2} - \frac{q^{2r-t-1}}{5}$.

If $h = 0$, then $|\mathcal{S}| = 0$, and if $h = 1$, then $|\mathcal{S}| \leqslant 1$. Therefore, we can restrict ourselves to the case $h \geqslant 2$. For $i \in \mathbb{N}$, let λ_i be the number of hyperplanes with i holes. By counting the number of hyperplanes on two different ways, it follows that

$$\sum_i \lambda_i = \frac{q^{d+1}-1}{q-1}. \tag{5.2.1}$$

Double counting of the pairs (H, P), where H is a hyperplane of $\mathcal{P}$ and where P is a hole incident with H, leads us to the identity

$$\sum_i i\lambda_i = \left(\frac{q^r-1}{q-1} + s\frac{q^{t+1}-1}{q-1}\right) \cdot \frac{q^d-1}{q-1}. \tag{5.2.2}$$

Furthermore, if we count the tuples (H, P_1, P_2), with a hyperplane H, two different holes P_1 and P_2, such that P_1 and P_2 are contained in the hyperplane H, we get

$$\sum_i i(i-1)\lambda_i = \left(\frac{q^r-1}{q-1} + s\frac{q^{t+1}-1}{q-1}\right) \cdot \left(\frac{q^r-1}{q-1} + s\frac{q^{t+1}-1}{q-1} - 1\right) \cdot \frac{q^{d-1}-1}{q-1}. \tag{5.2.3}$$

Since we know from Lemma 5.2.6 that the number of holes in a hyperplane is $\frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} \pmod{q^t}$, $\lambda_i = 0$ except for the cases when $i = \frac{q^r-1}{q-1} + s \cdot \frac{q^t-1}{q-1} + x \cdot q^t$ for a certain $x \in \mathbb{Z}$. This implies that

$$\sum_i \left(i - \frac{q^r-1}{q-1} - s \cdot \frac{q^t-1}{q-1}\right) \cdot \left(i - \frac{q^r-1}{q-1} - s \cdot \frac{q^t-1}{q-1} + q^t\right) \lambda_i \geqslant 0.$$

Indeed, if $\lambda_i \neq 0$, then the other two factors are just $x \cdot q^t$ and $(x+1) \cdot q^t$ for a certain x. So if the first factor is negative, then the second one is also negative or equals zero. Or if the first one is positive, then the second factor is positive.

Inserting the values of $\sum_i \lambda_i$, $\sum_i i\lambda_i$ and $\sum_i i(i-1)\lambda_i$, received from the identities (5.2.1), (5.2.2) and (5.2.3), and some calculations later ([14]), the assertion is proved.

The example of the partial t-spread with parameter $s = q^r - 1$ follows from Corollary 5.2.5. □

The previous theorem shows that Corollary 5.2.5 is sharp in the case $r = 1$. For $r > 1$, this theorem closes half of the gap between Corollary 5.2.5 and Theorem 5.2.2. Furthermore, it was conjectured that $s \geqslant q^r - 1$, so that there would be no examples of partial spreads with a size larger than the lower bound of Theorem 5.1.2. This would mean that in the case of a partial 2-spread $\mathcal{S}$ in $\mathrm{PG}(7, 2)$ (and so with the parameters $t = 2$, $h = 2, r = 2$), $|\mathcal{S}| \leqslant 33$. However, in [15] El-Zanati et al. showed that there is a partial 3-spread in the finite vector space $V(8, 2)$, which corresponds to a partial 2-spread in $\mathrm{PG}(7, 2)$, of size 34. Then, the parameter s in Theorem 5.2.7 for this case is 2. Now the question arises if it is possible that there exists a 3-spread of size 35. From Theorem 5.2.7 it follows that

$$s > \frac{2^2 - 1}{2} - \frac{2^{4-2-1}}{5} = \frac{11}{10} > 1,$$

so $s \geqslant 2$. Therefore, in this case, the bound of Theorem 5.2.7 is sharp and the example of [15] has the largest size and is definitely a maximal partial 2-spread in $\mathrm{PG}(7, 2)$.

In the next section we will construct a partial spread code based on the construction of Beutelspacher, of size $q^r \cdot \frac{q^{h(t+1)}-1}{q^{t+1}-1} - q^r + 1$. But the example of El-Zanati et al. implies that maybe we could use a larger partial 2-spread in $\mathrm{PG}(7, 2)$ and construct a larger $(n, M, 2k, k)$-code. This would lower the upper bound of Corollary 5.3.9.

Nevertheless, it is still difficult to obtain a clear view on the structure of the partial spread given in [15], or to generalize this for coding purposes. By a computer search, done by Peter Vandendriessche, it is possible to give a geometrical interpretation of the set of holes of this partial 2-spread in $\mathrm{PG}(7, 2)$ described in Example 2 in [15]. Since the number of points in $\mathrm{PG}(7, 2)$ is $2^8 - 1 = 255$ and every 2-dimensional subspace of the partial spread consists of 7 points, the number of holes is $255 - 7.34 = 17$. In the figure below, the following description of the 17 holes is visualised.

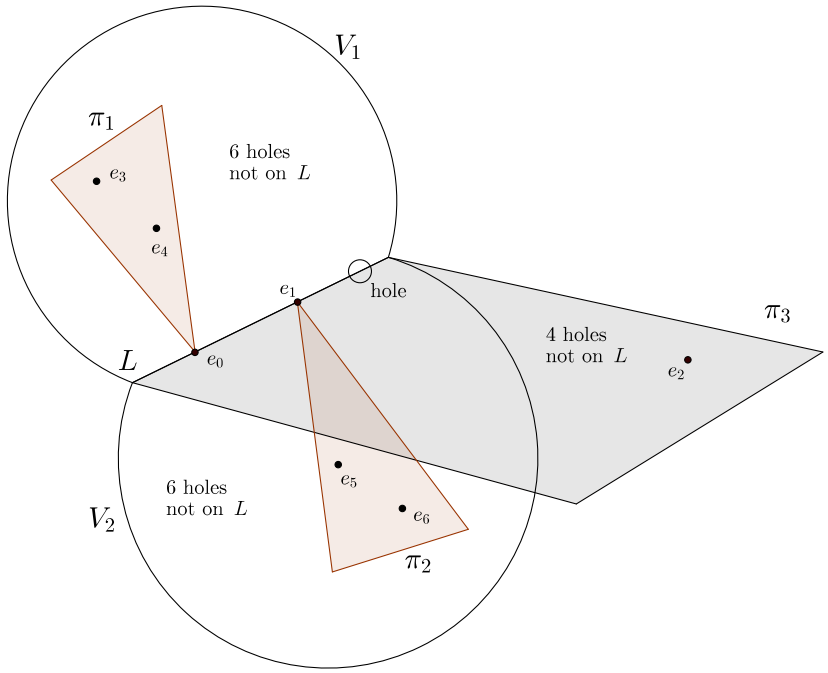


Figure 5.2: The set of holes for the maximal partial 2-spread of size 34 in $\mathrm{PG}(7, 2)$

Vandendriessche made a coordinatisation of PG$(7,2)$, where all points are of the form $(x_0,\ldots,x_7)$ and e_i are the points of the basis with coordinates $x_j=\delta_{ij}$, with δ_{ij} the Kronecker delta. He found that all holes lie in the hyperplane $X_7=0$, more specifically the holes are the points of 2 3-spaces $V_1=\langle e_0,e_1,e_3,e_4\rangle$ and $V_2=\langle e_0,e_1,e_5,e_6\rangle$ and one plane $\pi_3=\langle e_0,e_1,e_2\rangle$ through the line $L=\langle e_0,e_1\rangle$, except for the 14 points of the two planes $\pi_1=\langle e_0,e_3,e_4\rangle$ and $\pi_2=\langle e_1,e_5,e_6\rangle$ which lie respectively in V_1 and V_2.

Possibly, this example is just a 'Spielerei' and not very useful for decoding algorithms. Certainly we do not have this problem with the partial spread code $\mathscr{C}_q(k,n;p,p')$. In the next section, we construct this specific partial spread code, based on the idea of the construction of Corollary 5.2.5, and use the block structure of $\mathscr{C}_q(k,n;p,p')$, which allows us to produce an efficient decoding algorithm for partial spread codes.

Remark 5.2.8. In the case when $t+1$ is not a divisor of $d+1$, examining how many mutually disjoint t-dimensional subspaces we can put in a d-dimensional projective space, is a natural question. But also the question of the smallest number of t-dimensional subspaces which cover the whole projective space, rises up. This leads us to the concept of a t-cover. This is a set of t-dimensional subspaces of PG(d,q) which cover all of the points of PG(d,q). A t-cover is called minimal when no proper subset of it is still a t-cover. Taking again the article of Eisfeld and Storme ([14]), gives us a nice equivalence between t-covers in projective spaces and q-covering designs $\mathscr{C}_q(n,k,1)$, examined in e.g. Subsection 4.4.1. For example, Proposition 2.1 in [14] and Theorem 4.4.7 are basically the same. Although this subject is very interesting, we will not examine this further in this dissertation.

5.3 The partial spread code $\mathscr{C}_q(k,n;p,p')$

From the construction of Etzion and Vardy ([17]) used in Lemma 4.4.5 and Theorem 5.1.2, we obtain a partial spread code. The size of this code is

$$\frac{q^n-q^k(q^r-1)-1}{q^k-1}=\frac{q^n-q^r}{q^k-1}-q^r+1. \tag{5.3.1}$$

This is also the size of the partial t-spread constructed in the previous section (see Corollary 5.2.5). This construction can be related to another partial spread code, which we will present in this section, based on the article [21] of Gorla and Ravagnani. The advantage of this code is the ability to give an efficient decoding algorithm for these partial spread codes. We will present the ideas of this procedure in Subsection 5.3.2 after we have explained the construction and some interesting properties of this partial spread code, which will be denoted by $\mathscr{C}_q(k,n;p,p')$.

5.3.1 Construction and properties of $\mathscr{C}_q(k,n;p,p')$

The vector spaces of the partial spread we will construct, are given as row spaces of appropriate easy-computable matrices. For that, we introduce the following matrix.

Definition 5.3.1. Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Choose a primitive monic polynomial $p \in \mathbb{F}_q[x]$ of degree $k \geqslant 1$ and write $p = \sum_{i=0}^{k} p_i x^i$. Define the ***companion matrix of p*** by

$$M(p) \coloneqq \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \dots & -p_{k-1} \end{bmatrix}.$$

Now consider this situation and denote by P the companion matrix $M(p)$, then the following lemma holds, which is shown in Section 2.5 of [29].

Lemma 5.3.2. *The $\mathbb{F}_q$-algebra $\mathbb{F}_q[P]$ is a finite field with q^k elements.*

Before we present the construction of the partial spread code in Theorem 5.3.4, we start with an elementary lemma about vector spaces.

Lemma 5.3.3. *Let V be a finite-dimensional vector space over a field $\mathbb{F}$. Let $D \subseteq V$ be any subset, $\langle D \rangle$ the vector space spanned by the elements of this subset D, and set $d \coloneqq \dim_{\mathbb{F}} \langle D \rangle$[3]. Choose a finite subset $S \subseteq D$. Then*

$$\dim_{\mathbb{F}} \langle D \backslash S \rangle \geqslant d - |S|.$$

Proof. Since $D = (D \backslash S) \cup S$, it follows that $\langle D \backslash S \rangle + \langle S \rangle \supseteq \langle (D \backslash S) \cup S \rangle = \langle D \rangle$. From this, together with the Dimension theorem, we get

$$\begin{aligned} \dim_{\mathbb{F}} \langle D \backslash S \rangle + \dim \langle S \rangle &= \dim_{\mathbb{F}}(\langle D \backslash S \rangle + \langle S \rangle) + \dim_{\mathbb{F}}(\langle D \backslash S \rangle \cap \langle S \rangle) \\ &\geqslant \dim_{\mathbb{F}} \langle D \rangle + \dim_{\mathbb{F}}(\langle D \backslash S \rangle \cap \langle S \rangle) \\ &= d + \dim_{\mathbb{F}}(\langle D \backslash S \rangle \cap \langle S \rangle). \end{aligned}$$

Since $\dim_{\mathbb{F}}(\langle D \backslash S \rangle \cap \langle S \rangle) \geqslant 0$ and since $\dim_{\mathbb{F}} \langle S \rangle \leqslant |S|$ always holds, it follows that

$$\dim_{\mathbb{F}} \langle D \backslash S \rangle + |S| \geqslant \dim_{\mathbb{F}} \langle D \backslash S \rangle + \dim \langle S \rangle \geqslant d,$$

and so we can conclude that

$$\dim_{\mathbb{F}} \langle D \backslash S \rangle \geqslant d - |S|. \qquad \square$$

Theorem 5.3.4. *Consider the finite field $\mathbb{F}_q$ with q elements, q a prime power. Choose integers $1 \leqslant k < n$ and write $n = hk + r$ with $0 \leqslant r \leqslant k - 1$. Assume $h \geqslant 2$. Let $p, p' \in \mathbb{F}_q[x]$ be two primitive monic polynomials of degree k and $k + r$ respectively, and let $P \coloneqq M(p)$, $P' \coloneqq M(p')$ be their companion matrices. For any $1 \leqslant i \leqslant h - 1$ set*

$$\begin{aligned} \mathscr{M}_i(p, p') \coloneqq \{ \begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix} \mid \\ A_{i+1}, \dots, A_{h-1} \in \mathbb{F}_q[P], A \in \mathbb{F}_q[P'] \}, \end{aligned}$$

[3]For this lemma we emphasize the fact that we define the dimension over the field $\mathbb{F}$. In most cases, this is clear from the context and so, the subscript of the dimension will not be used.

where 0_k is the $(k \times k)$-matrix with zero entries, which appears $i-1$ times in $\mathscr{M}_i(p,p')$, I_k the $(k \times k)$-identity matrix, and $A_{(k)}$ denotes the last k rows of A.

The set

$$\mathcal{C} \coloneqq \bigcup_{i=1}^{h-1} \{\mathrm{rowsp}(M) : M \in \mathscr{M}_i(p,p')\} \cup \{\mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}\}$$

is a partial spread code in $\mathbb{F}_q^n$ of dimension k. In particular, the minimum distance of $\mathcal{C}$ is $2k$.

Proof. We have to prove that $\mathcal{C}$ is a set of k-dimensional subspaces of $\mathbb{F}_q^n$, whose pairwise intersections are trivial. So first take two different matrices $M_1 \in \mathscr{M}_i(p,p')$ and $M_2 \in \mathscr{M}_j(p,p')$, with $1 \leqslant i,j \leqslant h-1$. Define $V_1 \coloneqq \mathrm{rowsp}(M_1)$ and $V_2 \coloneqq \mathrm{rowsp}(M_2)$. By definition, we have $d(V_1,V_2) = 2k - 2\dim(V_1 \cap V_2)$, from which it follows that $d(V_1,V_2) = 2k$ if and only if

$$\mathrm{rk}\begin{bmatrix} M_1 \\ M_2 \end{bmatrix} = 2k.$$

To prove this for every $M_1 \neq M_2$, we have to look for a submatrix N of $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$, or of $\begin{bmatrix} M_2 \\ M_1 \end{bmatrix}$, of rank $2k$. First, if $i \neq j$, it is possible to find either in $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$, or in $\begin{bmatrix} M_2 \\ M_1 \end{bmatrix}$, a submatrix of the form

$$N_1 \coloneqq \begin{bmatrix} I_k & B \\ 0_k & I_k \end{bmatrix},$$

with $B \in \mathbb{F}_q[P]$. The rank of this matrix N_1 is $2k$. Now, consider the case where both M_1 and M_2 are matrices of $\mathscr{M}_i(p,p')$ for a fixed i. Then either

$$N_2 \coloneqq \begin{bmatrix} I_k & B_1 \\ I_k & B_2 \end{bmatrix}, \qquad \text{with } B_1 \neq B_2 \in \mathbb{F}_q[P],$$

or

$$N_3 \coloneqq \begin{bmatrix} I_k & X_{(k)} \\ I_k & Y_{(k)} \end{bmatrix}, \qquad \text{with } X \neq Y \in \mathbb{F}_q[P'],$$

will be a submatrix of $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$ or $\begin{bmatrix} M_2 \\ M_1 \end{bmatrix}$. The rank of N_2 is equal to the rank of the matrix

$$\begin{bmatrix} I_k & B_1 \\ 0_k & B_2 - B_1 \end{bmatrix}.$$

Since $B_1 \neq B_2$ and since we know from Lemma 5.3.2, that $\mathbb{F}_q[P]$ is a field, $B_1 - B_2$ is an invertible matrix. Therefore, $\mathrm{rk}(N_2) = 2k$.

In order to study the last case of the matrix N_3, consider the $(2(k+r) \times 2(k+r))$-matrix

$$H \coloneqq \begin{bmatrix} I_{k+r} & X \\ I_{k+r} & Y \end{bmatrix}.$$

Since $X \neq Y$, the same arguments as above lead us again to the fact that

$$\det \begin{bmatrix} I_{k+r} & X \\ 0_{k+r} & Y - X \end{bmatrix} = \det(X - Y) \neq 0,$$

so $\mathrm{rk}(H) = 2(k+r)$. Delete from H the rows from one to r and from $k+r+1$ to $k+2r$. We obtain a $2k \times 2(k+r)$ matrix, which we denote by $\tilde{H}$. The rows of this matrix $\tilde{H}$ are exactly the rows of N_3, except for the r extra zeroes in the beginning. In particular, $\mathrm{rk}(\tilde{H}) = \mathrm{rk}(N_3)$. By Lemma 5.3.3, we get $\mathrm{rk}(\tilde{H}) \geqslant 2(k+r) - 2r = 2k$, which implies that the rank of N_3 is also the required rank $2k$.

In order to complete the proof, we take the matrix $M_1 \in \mathscr{M}_i(p, p')$ and set $M_2 \coloneqq \begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. Also in this case, it follows that

$$\mathrm{rk} \begin{bmatrix} M_1 \\ M_2 \end{bmatrix} = 2k.$$

□

Remark 5.3.5. We already mentioned that the construction of the partial spread code of Theorem 5.3.4 is based on the ideas of the construction of Beutelspacher in Theorem 5.2.4 and Corollary 5.2.5, visualised in Figure 5.1 with the 'slices'. This connection can be seen in the following way. First, note that the parameter k in the case of vector spaces in this section corresponds to the parameter $t+1$ used in Section 5.2 and parameter h is the same. The element rowsp $\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$ of the partial spread code $\mathcal{C}$ of Theorem 5.3.4 corresponds to the special element of the partial t-spread $\mathcal{S}$ in the fixed $(r+t)$-dimensional subspace of $\mathcal{P}$, i.e. the element $[t]$ in the projective space $PG(t+r, q)$ in Figure 5.1. Furthermore, if we take another element of $\mathcal{C}$, this element is the rowspace of a matrix $M \in \mathscr{M}_i(p, p')$ for a fixed i, so M is of the form

$$\begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix},$$

with $A_{i+1}, \ldots, A_{h-1} \in \mathbb{F}_q[P], A \in \mathbb{F}_q[P']$. We associate such an element with an element of a spread obtained when we apply Lemma 5.2.3 for parameter $s = (h-i)(t+1) + r - 1$, as we did in the proof of Theorem 5.2.4. This is an element in the projective space $PG((h-i+1)(t+1) + r - 1, q)$ (see also Figure 5.1).

Definition 5.3.6. The partial spread code $\mathcal{C}$ defined in the statement of Theorem 5.3.4 will be denoted by $\mathscr{C}_q(k, n; p, p')$. Since for any (n, M, d)-code $\mathcal{C}$ in projective space, the complementary code $\mathcal{C}^\perp$ is also an (n, M, d)-code, as noted in Subsection 2.2.3, we may assume $k \leqslant \frac{n}{2}$.

In the next example, we construct such a partial spread code $\mathscr{C}_q(k, n; p, p')$ of length $n = 7$ and dimension $k = 2$ over the binary field $\mathbb{F}_2$.

Example 5.3.7. First observe that, with the parameters $(q, n, k) = (2, 7, 2)$, it follows that $n \equiv 1 \pmod{k}$. Therefore, in the notation of Theorem 5.3.4, $r = 1$ and $h = 3$. Take the primitive monic polynomials $p(x) \coloneqq x^2 + x + 1$, $p'(x) \coloneqq x^3 + x + 1 \in \mathbb{F}_2[x]$.

Theorem 5.3.4 assures that from these polynomials, we can construct a partial spread code $\mathscr{C}_2(2,7;p,p')$. From Definition 5.3.1, the companion matrices of p and p' are

$$P := M(p) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad \text{and} \qquad P' := M(p') = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

This implies that the elements of $\mathscr{C}_2(2,7;x^2+x+1,x^3+x+1)$ are the row spaces of all the matrices in the following forms:

$$\begin{bmatrix} 1 & 0 & A_1 & A_{(2)} \\ 0 & 1 & & \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 & 0 & B_{(2)} \\ 0 & 0 & 0 & 1 & \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where A_1 is any matrix in $\mathbb{F}_q[P]$ and $A_{(2)}$, $B_{(2)}$ denote the last two rows of any arbitrary $A, B \in \mathbb{F}_q[P']$.

From Lemma 5.3.2 and Theorem 5.3.4, it follows that the number of elements of the code constructed in this example is $2^2 \cdot 2^3 + 2^3 + 1 = 41$. The size of a partial spread code $\mathscr{C}_q(k,n;p,p')$ will be generalized in the following theorem. This will be indeed the size (5.3.1), suggested in the beginning of this section.

Theorem 5.3.8. *Let $\mathcal{C}$ be a partial spread code $\mathscr{C}_q(k,n;p,p')$. Then the cardinality of $\mathcal{C}$ is*

$$|\mathcal{C}| = \frac{q^n - q^r}{q^k - 1} - q^r + 1.$$

Proof. Note that we follow the notation of Theorem 5.3.4. The matrices in the statement of Theorem 5.3.4 are given in row-reduced echelon form, which is canonical (see e.g. Section 2.2 of [32]). Furthermore, we will prove that for two different matrices $X, Y \in \mathbb{F}_q[P']$, also the matrices of the last k rows, i.e. $X_{(k)}$ and $Y_{(k)}$, are different. Indeed, assume to the contrary that $X_{(k)} = Y_{(k)}$ for arbitrary matrices $X, Y \in \mathbb{F}_q[P']$, $X \neq Y$. We have

$$\operatorname{rk} \begin{bmatrix} I_{k+r} & X \\ I_{k+r} & Y \end{bmatrix} = 2(k+r).$$

The same technique as in the proof of Theorem 5.3.4 with the matrix H, where we deleted from the matrix the rows from one to r and from $k+r+1$ to $k+2r$, shows that

$$\operatorname{rk} \begin{bmatrix} I_k & X_{(k)} \\ I_k & Y_{(k)} \end{bmatrix} = 2k.$$

But since $X_{(k)} = Y_{(k)}$, this is a contradiction, so it follows that $X = Y$. By Lemma 5.3.2 and since the sum of the first $h-1$ terms of a geometric series is $\sum_{i=0}^{h-2} a^i = \frac{a^{h-1}-1}{a-1}$, the size of $\mathcal{C}$ can be computed, as

$$|\mathcal{C}| = q^{k+r} \sum_{i=0}^{h-2} q^{ki} + 1 = q^{k+r} \frac{q^{n-r-k} - 1}{q^k - 1} + 1 = \frac{q^n - q^r}{q^k - 1} - q^r + 1. \qquad \square$$

Combining Theorem 5.1.4 and Theorem 5.3.8, gives us the following corollary.

Corollary 5.3.9. *Let $\mathcal{C}$ be a partial spread code $\mathscr{C}_q(k,n;p,p')$ and let r be the remainder obtained dividing n by k. Then*

$$\mathcal{A}_q(n,2k,k) - |\mathcal{C}| \leqslant q^r - 1.$$

If $r = 1$, Theorem 5.2.7 implies that this bound is sharp. Nevertheless, for the case of $n = 8$ and $k = 3$ (and therefore $r = 2$), this is not true. Indeed, it follows from the example of El-Zanati et al. ([15]), discussed at the end of Subsection 5.2, that $\mathcal{A}_q(8,6,3) = 34$, and therefore $\mathcal{A}_q(n,2k,k) - |\mathcal{C}| = 34 - 33 = 1 < 2^2 - 1$.

When constructing partial spread codes, it is always the goal to achieve a spread code with a size as large as possible. This means that we want to extend a given partial spread code. When this is not possible anymore, we call this partial spread code maximal (see Definition 5.1.3). From Corollary 5.3.9, it follows that there is still room for improvement, if $r > 1$. Nevertheless, the following theorem ensures that $\mathscr{C}_q(k,n;p,p')$ cannot be improved as an $(n,M,2k,k)$-code by adding new codewords.

Theorem 5.3.10. *Let $\mathcal{C}$ be a partial spread code $\mathscr{C}_q(k,n;p,p')$. Then $\mathcal{C}$ is a maximal code contained in $\mathcal{G}_q(n,k)$ of minimum distance $2k$, with respect to inclusion.*

Proof. We have to prove that there is no partial k-spread $\mathcal{C}'$ in $\mathbb{F}_q^n$ such that $\mathcal{C} \subseteq \mathcal{C}'$ and $|\mathcal{C}| < |\mathcal{C}'|$. Write, as in Theorem 5.3.4, $n = hk + r$ with $0 \leqslant r < k$ and we can assure that $h \geqslant 2$, because of the assumption in Definition 5.3.6 that $k \leqslant \frac{n}{2}$. Define the partial k-spread

$$\overline{\mathcal{C}} \coloneqq \mathcal{C} \backslash \{\text{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}\}.$$

Assume, by contradiction, that there exists a partial k-spread $\mathcal{C}'$ in $\mathbb{F}_q^n$ such that $\mathcal{C}' \supseteq \overline{\mathcal{C}}$ and $|\mathcal{C}'| \geqslant |\overline{\mathcal{C}}| + 2$. Denote by S the set of vectors $\cup\overline{\mathcal{C}}\backslash\{0\}$. From Theorem 5.3.8 we know that $|\overline{\mathcal{C}}| = \frac{q^n - q^r}{q^k - 1} - q^r$ and hence,

$$|S| = (q^k - 1) \cdot |\overline{\mathcal{C}}| = q^n - q^{k+r}.$$

The set $X \coloneqq \{x \in \mathbb{F}_q^n \,|\, x_i = 0 \text{ for any } i = 1, \ldots, (h-1)k\}$ is a $(k+r)$-dimensional subspace of $\mathbb{F}_q^n$. Since one of the $(k \times k)$-submatrices of an element of $\mathscr{M}_i(p,p')$, with $1 \leqslant i \leqslant h-1$, is always a $(k \times k)$-identity matrix, every vector of S has always at least one nonzero coordinate x_i, $1 \leqslant i \leqslant (h-1)k$. This implies the inclusion $X \subseteq \mathbb{F}_q^n \backslash S$ and therefore,

$$|\mathbb{F}_q^n \backslash S| = q^n - (q^n - q^{k+r}) = q^{k+r} = |X|.$$

Consequently, $X = \mathbb{F}_q^n \backslash S$ and so $\mathbb{F}_q^n$ is the union of the disjoint sets X and S. For every $s \in S$, there exists exactly one subspace $V_s \in \overline{\mathcal{C}}$ such that $s \in V_s$. Therefore, since $\mathcal{C}' \supseteq \mathcal{C} \supseteq \overline{\mathcal{C}}$, with $|\mathcal{C}'| \geqslant |\overline{\mathcal{C}}| + 2$, there are at least two codewords V_1 and V_2 of $\overline{\mathcal{C}}$, such that $V_1 \cap V_2 = \{0\}$ and $V_1, V_2 \subseteq X$. Since X is a vector space containing both V_1 and V_2, we have the inclusion $V_1 + V_2 \subseteq X$. This implies the inequality

$$\dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2) \leqslant \dim(X),$$

which leads to the contradiction $2k \leqslant k + r$. □

Theorem 5.3.10 tells us that we cannot extend $\mathscr{C}_q(k,n;p,p')$ to a larger partial spread code. Although we already noted that the counter example of El-Zanati et al. ([15]) shows that the bound in Corollary 5.3.9 is not always sharp, it is hard to find a useful interpretation of the elements of this specific partial spread seen as a rowspace of some matrices with a block structure. Therefore, one has doubts about the applications and generalisations for decoding purpose. Nonetheless, the case of the partial spread codes $\mathscr{C}_q(k,n;p,p')$ is very suitable for this. In the last subsection of this thesis, we explain some key elements to a successful decoding algorithm for this partial spread codes $\mathscr{C}_q(k,n;p,p')$.

5.3.2 Towards a decoding algorithm for partial spread codes

First we start this subsection with an investigation of the block structure of the partial spread code defined in Theorem 5.3.4.

Theorem 5.3.11. *Let $\mathcal{C}$ be a partial spread code $\mathscr{C}_q(k,n;p,p')$ and let $V \in \mathcal{C}$ be a codeword, say*

$$V \coloneqq \operatorname{rowsp}\begin{bmatrix} S_1 & \cdots & S_{h-1} & S \end{bmatrix},$$

where the matrices S_i are $(k \times k)$-matrices and where S is a $(k \times (k+r))$-matrix. Let $X \subseteq \mathbb{F}_q^n$ be a t-dimensional vector subspace defined by

$$X \coloneqq \operatorname{rowsp}\begin{bmatrix} M_1 & \cdots & M_{h-1} & M \end{bmatrix},$$

where the matrices M_i are $(k \times k)$-matrices and M is a $(k \times (k+r))$-matrix. If $d(V,X) < k$, then X decodes to V. Moreover, for any $1 \leqslant i \leqslant h-1$, the following two facts are equivalent:

(i) $S_i = 0_k$,

(ii) $\operatorname{rk}(M_i) \leqslant \frac{t-1}{2}$.

Proof. From Theorem 5.3.4 we know that the minimum distance of $\mathcal{C}$ is $2k$. If $d(V,X) < k$, a minimum-distance decoder will decode the subspace X as the codeword V (see also Subsection 2.2.4). Indeed, if the minimum-distance decoder would return another codeword $U \in \mathcal{C}$, then $d(U,X) \leqslant d(V,X) < k$ and hence, applying the triangle inequality,

$$d(U,V) \leqslant d(U,X) + d(X,V) < 2k,$$

which gives a contradiction.

(i)⇒(ii): We will first prove that, for an arbitrary i, $1 \leqslant i \leqslant h-1$, if $S_i = 0_k$, then $\operatorname{rk}(M_i) \leqslant \frac{t-1}{2}$.

Without loss of generality, we assume that the matrix $\begin{bmatrix} S_1 & \cdots & S_{h-1} & S \end{bmatrix}$ is in row-reduced echelon form. We assume that $S_i = 0_k$. By the definition of $\mathcal{C}$, then

(a) either there exists an index j, $1 \leqslant j \leqslant h-1$ with $j \neq i$, such that $S_j = I_k$, or

(b) $S_j = 0_k$ for any $1 \leqslant j \leqslant h-1$.

In the first case (a), define the matrix M_{ij} by

$$M_{ij} \coloneqq \begin{bmatrix} 0_k & I_k \\ M_i & M_j \end{bmatrix}.$$

The rank of this matrix is upper bounded by $\dim(V+X)$. Since $d(V,X) < k$, by definition, $\dim(V)+\dim(X)-2\dim(V\cap X) < k$ or equivalently $\dim(V\cap X) > \frac{t}{2}$. This implies that

$$\mathrm{rk}(M_{ij}) \leqslant \dim(V+X) = k+t-\dim(V\cap X) < k+\frac{t}{2}. \tag{5.3.2}$$

Therefore, it follows that

$$\mathrm{rk}(M_{ij}) = k+\mathrm{rk}(M_i) < k+\frac{t}{2},$$

and hence,

$$\mathrm{rk}(M_i) \leqslant \frac{t-1}{2}.$$

In the latter case (b), by the definition of $\mathcal{C}$, we have $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. We will use the same technique as above. Define the matrix

$$M_{ij} \coloneqq \begin{bmatrix} 0_k & 0_{k\times r} I_k \\ M_i & M \end{bmatrix}.$$

Again, we have the inequality (5.3.2), and so we get

$$\mathrm{rk}(M_{ij}) = k+\mathrm{rk}(M_i) < k+\frac{t}{2},$$

from which it follows also that $\mathrm{rk}(M_i) \leqslant \frac{t-1}{2}$.

(ii)⇒(i): Assuming that $\mathrm{rk}(M_i) \leqslant \frac{t-1}{2}$, we will now prove that $S_i = 0_k$.

If we assume, by contradiction, that $S_i \neq 0_k$ then, by the definition of $\mathcal{C}$ and Lemma 5.3.2, all the nonzero matrices of $\mathbb{F}_q[P]$ are invertible, and therefore $\mathrm{rk}(S_i) = k$. Denote by $\pi\colon \mathbb{F}_q^n \to \mathbb{F}_q^k$ the projection on the coordinates $ki+1, ki+2, \ldots, k(i+1)$. Since $\pi(V) = \mathrm{rowsp}(S_i)$ and $\mathrm{rk}(S_i) = k$, it follows that $\pi_{|V}$ is surjective. Since $\dim(V) = k$, we get that $\pi_{|V}$ is also injective. The inclusion $\pi(V\cap X) \subseteq \pi(V)\cap\pi(X)$ follows from the fact that if we take an element of $\pi(V\cap X)$, this is the projection of an element y, such that $y \in V$ and $y \in X$, and so $\pi(y)$ is an element of $\pi(V)$ and of $\pi(X)$. Therefore, we have $\dim(\pi(V\cap X)) \leqslant \dim(\pi(V)\cap\pi(X))$ and so

$$\dim(V\cap X) = \dim(\pi(V\cap X)) \leqslant \dim(\pi(V)\cap\pi(X)) \leqslant \dim(\pi(X)) = \mathrm{rk}(M_i) \leqslant \frac{t-1}{2}.$$

This implies that $\dim(V)+\dim(X)-2\dim(V\cap X) \geqslant k+t-(t-1)$, which contradicts the assumption that $d(V,X) < k$. □

The previous theorem has the following useful interpretation. Suppose we use a partial spread code $\mathcal{C} \coloneqq \mathscr{C}_q(k,n;p,p')$ for random network coding and suppose that we receive a t-dimensional vector space $X \coloneqq \mathrm{rowsp}\begin{bmatrix} M_1 & \cdots & M_{h-1} & M \end{bmatrix}$. Assume that there exists

a codeword $V \in \mathcal{C}$ such that $d(V, X) < k$, then the minimum-distance decoder will return V, as stated in Theorem 5.3.11. If $\mathrm{rk}(M_i) \leqslant \frac{t-1}{2}$ for any i, $1 \leqslant i \leqslant h-1$, then $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. Otherwise, denote by i the smallest integer $1 \leqslant i \leqslant h-1$, such that $\mathrm{rk}(M_i) > \frac{t-1}{2}$. Then there exist unique matrices $A_{i+1}, \ldots, A_{h-1} \in \mathbb{F}_q[P]$ and a unique matrix $A \in \mathbb{F}_q[P']$ such that $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix}$, where the identity matrix I_k is the ith $(k \times k)$-block. To find these block matrices, we will need a decoding algorithm. To reduce the complexity of the algorithm, the following theorem is very useful.

Theorem 5.3.12. *With the setting described above and assuming that the codeword* $V \neq \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$, *then, for any* $i+1 \leqslant j \leqslant h-1$, *we have*

$$d(\mathrm{rowsp}\begin{bmatrix} I_k & A_j \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M_j \end{bmatrix}) < k$$

and

$$d(\mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M \end{bmatrix}) < k.$$

Proof. Fix an integer j such that $i+1 \leqslant j \leqslant h-1$ and denote this time by $\pi\colon \mathbb{F}_q^n \to \mathbb{F}_q^{2k}$ the projection on the coordinates $ki+1, ki+2, \ldots, k(i+1), kj+1, kj+2, \ldots, k(j+1)$. Since $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix}$, where the identity matrix I_k is the i-th $(k \times k)$-block, it follows that $\pi(V) = \mathrm{rowsp}\begin{bmatrix} I_k & A_j \end{bmatrix}$. In particular, $\dim(\mathrm{im}\,\pi_{|V}) = \mathrm{rk}(\pi_{|V}) = k$. From the identity $\dim(\mathrm{im}\,\pi_{|V}) + \dim(\ker \pi_{|V}) = \dim(V)$, it follows that $\dim(\ker \pi_{|V}) = 0$, which means that $\pi_{|V}$ is injective. Therefore, we have $\dim(\pi(V \cap X)) = \dim(V \cap X)$. Furthermore, $\pi(X) = \mathrm{rowsp}\begin{bmatrix} M_i & M_j \end{bmatrix}$ and we have the inclusion $\pi(V \cap X) \subseteq \pi(V) \cap \pi(X)$, so $\dim(\pi(V \cap X)) \leqslant \dim(\pi(V) \cap \pi(X))$. Hence,

$$\begin{aligned} d(\mathrm{rowsp}\begin{bmatrix} I_k & A_j \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M_j \end{bmatrix}) &= d(\pi(V), \pi(X)) \\ &= \dim(\pi(V)) + \dim(\pi(X)) - 2\dim(\pi(V) \cap \pi(X)) \\ &\leqslant k + t - 2\dim(\pi(V \cap X)) \\ &= k + t - 2\dim(V \cap X) \\ &= d(V, X) \\ &< k. \end{aligned}$$

Doing an analogous proof with the function $\pi\colon \mathbb{F}_q^n \to \mathbb{F}_q^{2k+r}$ as the projection on the coordinates $ki+1, ki+2, \ldots, k(i+1), k(h-1)+1, k(h-1)+2, \ldots, kh, kh+1, \ldots, kh+r$, will give us that $d(\mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M \end{bmatrix}) < k$. □

This theorem gives us the key to reduce decoding partial spread codes $\mathscr{C}_q(k, n; p, p')$ to decoding such partial spread codes for the cases $n = 2k$ and $n = 2k + r$, with $1 \leqslant r \leqslant h-1$. Moreover, the theorem allows us to parallellize the computation, which will decrease the decoding complexity to the case $n = 2k + r$. So, in order to decode a partial spread code $\mathscr{C}_q(k, n; p, p')$, we may restrict to decoding partial spread codes of the form $\mathscr{C}_q(k, 2k + r; p, p')$, with $0 \leqslant r \leqslant k-1$.

Remark 5.3.13. In the construction of Theorem 5.3.4 for a particular partial spread code $\mathscr{C}_q(k, 2k + r, p, p')$ with $0 \leqslant r \leqslant k-1$, we do not need the companion matrix of p. Therefore, we write $\boldsymbol{\mathscr{C}_q(k, 2k + r; p')}$.

For the case $r = 0$, we rely on the literature and do not work this out in this dissertation. For instance, in [28], there are decoding algorithms of the Reed-Solomon like codes and in [38] a decoding algorithm for Desarguesian spread codes is represented. Suppose that we have a t-dimensional row space X of a $(k \times 2k)$-matrix $\begin{bmatrix} M_1 & M_2 \end{bmatrix}$, assuming that X is decodable, i.e. assuming that there exists a codeword $V \in \mathscr{C}_q(k, 2k; p)$ such that $d(V, X) < k$. If $\mathrm{rk}(M_1) \leqslant \frac{t-1}{2}$, then $V = \begin{bmatrix} 0_k & I_k \end{bmatrix}$ (see the interpretation of Theorem 5.3.11). Otherwise, we can use a decoding algorithm for e.g. Reed-Solomon like codes on $\mathscr{C}_q(k, 2k; p) \backslash \{\mathrm{rowsp} \begin{bmatrix} 0_k & I_k \end{bmatrix}\}$, which returns a matrix in row-reduced form whose row space is the unique codeword $V \in \mathscr{C}_q(k, 2k; p)$ for which $d(V, X) < k$. This discussion leads to the following algorithm.

Data: A decodable t-dimensional row space X of a $(k \times 2k)$-matrix $\begin{bmatrix} M_1 & M_2 \end{bmatrix}$
Result: The unique $V \in \mathscr{C}_q(k, 2k; p)$ such that $d(V, X) < k$, given as a matrix in row-reduced echelon form whose row space is V;
if $\mathrm{rk}(M_1) \leqslant \frac{t-1}{2}$ **then**
  $V = \mathrm{rowsp} \begin{bmatrix} 0_k & I_k \end{bmatrix}$;
else
  Use a decoding algorithm for Reed-Solomon like codes on $\mathscr{C}_q(k, 2k; p) \backslash \{\mathrm{rowsp} \begin{bmatrix} 0_k & I_k \end{bmatrix}\}$;
end

Algorithm 1: Decoding a $\mathscr{C}_q(k, 2k; p)$ code

Now we focus on a decoding algorithm for partial spread codes of the form $\mathscr{C}_q(k, 2k+r; p)$, with $1 \leqslant r \leqslant k-1$. In the following theorem, we will construct a canonical embedding of a partial spread code $\mathscr{C}_q(k, 2k+r; p)$ into the spread code $\mathscr{C}_q(k+r, 2(k+r); p)$. In fact, this can be interpretated as a reverse construction of the construction of Beutelspacher in Corollary 5.2.5, as we did in Remark 5.3.5. From this embedding, a decoding algorithm for $\mathscr{C}_q(k+r, 2(k+r); p)$ (see Algorithm 1) will give a decoding algorithm for $\mathscr{C}_q(k, 2k+r; p)$.

Theorem 5.3.14. *Let $\mathcal{C}$ be a partial spread code $\mathscr{C}_q(k, 2k+r; p)$ with $1 \leqslant r \leqslant k-1$. Denote by X the t-dimensional vector space* $\mathrm{rowsp} \begin{bmatrix} M_1 & M \end{bmatrix}$ *in $\mathbb{F}_q^{2k+r}$, where M_1 is a $(k \times k)$-matrix and M a $(k \times (k+r))$-matrix. Assume the existence of a matrix $A \in \mathbb{F}_q[P]$ such that $d(\mathrm{rowsp} \begin{bmatrix} I_k & A_{(k)} \end{bmatrix}, \mathrm{rowsp} \begin{bmatrix} M_1 & M \end{bmatrix}) < k$. Now define the following two $((k+r) \times (k+r))$-matrices:*

$$\overline{M_1} := \begin{bmatrix} 0_r & 0_{r \times k} \\ 0_{k \times r} & M_1 \end{bmatrix} \quad \text{and} \quad \overline{M} := \begin{bmatrix} 0_{r \times (k+r)} \\ M \end{bmatrix}.$$

Then

$$d(\mathrm{rowsp} \begin{bmatrix} I_{k+r} & A \end{bmatrix}, \mathrm{rowsp} \begin{bmatrix} \overline{M_1} & \overline{M} \end{bmatrix}) < k + r.$$

Proof. Set $V := \mathrm{rowsp} \begin{bmatrix} I_k & A_{(k)} \end{bmatrix}$ and observe that

$$d(V, X) = \dim(V) + \dim(X) - 2\dim(V \cap X) < k$$

is equivalent to the fact that $d(V \cap X) > \frac{t}{2}$. Now define the following vector spaces:

$$\overline{V} := \mathrm{rowsp} \begin{bmatrix} I_{k+r} & A \end{bmatrix} \quad \text{and} \quad \overline{X} := \begin{bmatrix} \overline{M_1} & \overline{M} \end{bmatrix}.$$

By construction, $\dim(X) = \dim(\overline{X}) = t$ and $\dim(\overline{V} \cap \overline{X}) \geqslant \dim(V \cap X)$. Therefore, it follows that

$$\begin{aligned} d(\overline{V}, \overline{X}) &= \dim(\overline{V}) + \dim(\overline{X}) - 2\dim(\overline{V} \cap \overline{X}) \\ &= k + r + t - 2\dim(\overline{V} \cap \overline{X}) \\ &\leqslant k + r + t - 2\dim(V \cap X) \\ &< k + r + t - 2 \cdot \frac{t}{2} \\ &= k + r. \end{aligned}$$

□

The previous theorem has a useful application. In fact, it is the key to success for a decoding procedure for a partial spread code $\mathscr{C}_q(k, 2k + r; p)$, with $1 \leqslant r \leqslant k - 1$, using a decoding algorithm for $\mathscr{C}_q(k + r, 2(k + r); p)$. We will discuss this briefly below.

With the conditions of Theorem 5.3.14, assume $X := \text{rowsp}\begin{bmatrix} M_1 & M \end{bmatrix}$ is received. If $\text{rk}(M_1) \leqslant \frac{t-1}{2}$ then, again because of Theorem 5.3.11, $V = \begin{bmatrix} 0_k & 0_{k\times r} & I_k \end{bmatrix}$ will be the matrix of the corresponding codeword of $\mathscr{C}_q(k, 2k + r; p)$ returned by the decoding algorithm. Otherwise, we may construct the matrices $\overline{M_1}$ and $\overline{M}$ as described in Theorem 5.3.14 and obtain the vector space $\overline{X} := \begin{bmatrix} \overline{M_1} & \overline{M} \end{bmatrix}$. The minimum distance of the spread code $\mathscr{C}_q(k + r, 2(k + r); p)$ is $2(k + r)$. By Theorem 5.3.14, if X decodes to $V := \text{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}$ in $\mathscr{C}_q(k, 2k + r; p)$, then $\overline{X}$ decodes to $\overline{V} := \text{rowsp}\begin{bmatrix} I_{k+r} & A \end{bmatrix}$ in $\mathscr{C}_q(k+r, 2(k+r); p)$. Using the procedure[4] explained in Algorithm 1 for the spread code $\mathscr{C}_q(k+r, 2(k+r); p)$, applied to $\overline{X}$, it will produce $\begin{bmatrix} I_{k+r} & A \end{bmatrix}$. Finally, V is the rowspace of the matrix obtained by deleting the first r rows and the first r columns of $\begin{bmatrix} I_{k+r} & A \end{bmatrix}$. We summarize this procedure in the following algorithm.

Data: A decodable t-dimensional row space X of a $(k \times 2k + r)$-matrix $\begin{bmatrix} M_1 & M \end{bmatrix}$
Result: The unique $V \in \mathscr{C}_q(k, 2k; p)$ such that $d(V, X) < k$, given as a matrix in row-reduced echelon form whose row space is V;
if $\text{rk}(M_1) \leqslant \frac{t-1}{2}$ **then**
  $V = \text{rowsp}\begin{bmatrix} 0_k & 0_{k\times r} & I_k \end{bmatrix}$;
else
  Construct the matrix $\begin{bmatrix} \overline{M_1} & \overline{M} \end{bmatrix}$ as explained in Theorem 5.3.14;
  Use Algorithm 1 with $\mathscr{C}_q(k + r, 2(k + r); p)$ on $\begin{bmatrix} \overline{M_1} & \overline{M} \end{bmatrix}$;
  Delete the first r rows and the first r columns of the output;
end

Algorithm 2: Decoding a $\mathscr{C}_q(k, 2k + r; p)$ code, with $1 \leqslant r \leqslant k - 1$

[4] It is of course allowed to use any other decoding algorithm for spread codes.

Appendix Nederlandstalige samenvatting

Ongeveer een jaar geleden ging ik te rade bij Prof. Dr. Leo Storme voor een mogelijk onderwerp voor mijn masterproef. Hierbij ging mijn voorkeur vooral uit naar iets in de codeertheorie of meetkunde, en nog het liefst een combinatie van beide. Hij stelde me voor om het artikel van Kötter and Kschischang [28] over *random network coding* eens door te nemen. In dit bekroonde artikel wordt een netwerk beschouwd waarbij we de informatie niet halen uit de vectoren die worden doorgestuurd, maar waarbij we kijken naar de vectorruimten die deze vectoren opspannen. Op die manier zullen alle ontvangers meer informatie van alle verzenders kunnen ontvangen. Dit zal leiden tot een nieuw soort codeertheorie, gebruikmakende van de zogenaamde *subspace distance*. Dit artikel heeft een enorme stimulans gegeven aan het onderzoek rond random network coding en heeft ook mij kunnen overtuigen om mij hierin te verdiepen.

Random network coding, ook netwerk codering genoemd, heeft ook vele toepassingen in communicatienetwerken zoals het Internet, draadloze communicatiesystemen en cloud computing, en er zijn wereldwijd al vele werkgroepen die hiermee bezig zijn. Hierbij vermeld ik graag COST Action IC1104 (zie [9] of [10]), die een onderzoeksnetwerk over *random network coding and designs over* $\mathbb{F}_q$ hebben opgericht om met experten uit domeinen zoals zuivere en toegepaste wiskunde, computerwetenschappen en ingenieurswetenschappen, samen hierop te werken. Zo organiseerden zij in februari een eerste Europese trainingsschool over netwerk codering, waarbij ik het geluk had om hieraan te mogen deelnemen. Zo konden de interessante voordrachten en nuttige praktijksessies met experten uit dit vakgebied zoals Kschischang en Etzion, mij een beter en breder beeld geven over de mogelijkheden van dit onderwerp, en vooral veel motivatie en inspiratie om hiermee door te gaan.

Het resultaat van mijn ontdekkingstocht in een stukje van de wondere wereld van netwerk codering en q-designs schreef ik neer in deze thesis, waarvan ik nu kort de verschillende hoofdstukken zal toelichten.

In het eerste hoofdstuk *Preliminaries* worden alle belangrijke begrippen geïntroduceerd die nodig zijn voor het vervolg van de masterproef. Het doel van de inleiding is ook om later het verband te kunnen leggen met de begrippen, stellingen en bewijzen uit de klassieke codeertheorie, designtheorie en grafentheorie. Veel nieuwe zaken zijn namelijk q-analogons, waarbij de klassieke concepten verkregen worden uit de nieuwe door het nemen van de limiet voor $q \to 1$.

Bij het tweede hoofdstuk *Coding for errors and erasures in random network coding* gaan we van start met een algemene beschrijving van een netwerk, lineaire network codering, enzomeer. Hierbij vertrekken we van het idee van het *Butterfly network* en beschouwen we een kanaal waarbij de in- en output telkens deelruimten zijn van een overkoepelende

vectorruimte. Hierbij definiëren we een geschikte metriek en andere basisbegrippen. Zo komen we tot het begrip van een (n, M, d)-code in de projectieve ruimte. Ondanks deze naam, werken we echter voornamelijk met vectorruimten in plaats van projectieve ruimten. Het is verder niet onnatuurlijk om een speciale groep van codes te beschouwen, i.e. constante-dimensie codes, (n, M, d)-codes waarbij elk codewoord dezelfde dimensie k heeft en die leven in de Grassmanniaan $\mathcal{G}_q(n, k)$. Ten slotte onderzoeken we in welke mate random network codes *error*- en *erasure*-verbeterend zijn, i.e. in welke mate ze fouten en blanco's kunnen opvangen.

In het derde hoofdstuk over *Bounds on codes in random network coding* beschouwen we het 'hoofdprobleem van de codeertheorie' en gaan we op zoek naar de maximale waarde voor het aantal codewoorden in een n-dimensionale ruimte en met minimumafstand d. Daarbij is het natuurlijk om op zoek te gaan naar grenzen voor deze waarden. Vooreerst beschouwen we de grenzen voor constante-dimensie codes. Hierbij geven we het q-analogon van bijvoorbeeld de bolpakkingsgrens, bolbedekkingsgrens en Singleton grens. Daarnaast komen ook nog andere (betere) grenzen aan bod en beschouwen we kort het geval voor grenzen in het algemene geval van (n, M, d)-codes. Ook wordt in de laatste sectie uitvoerig ingegaan op het niet-bestaan van niet-triviale perfecte codes in de Grassmanniaan en in de projectieve ruimte.

Sterk gerelateerd met codes zijn designs. Daarom definiëren we in het vierde hoofdstuk *Designs over* $\mathbb{F}_q$ covering designs $\mathscr{C}_q(n, k, t)$, Turán designs $\mathscr{T}_q(n, k, t)$ en Steiner structuren $\mathscr{S}_q(t, k, n)$ en bespreken we hun bestaan en de grenzen op hun grootte voor verschillende parameters. Aangezien Steiner structuren optimale covering designs zijn, krijgen zij de meeste aandacht. Hierbij bespreken we het recente en belangrijke resultaat van [5] over het bestaan van Steiner structuren $\mathscr{S}_2(2, 3, 13)$ en bijgevolg het bestaan van Steiner systemen $\mathcal{S}(3, 8, 8192)$.

In het laatste hoofdstuk *Partial spreads and partial spread codes in random network coding* worden (partiële) spreads en (partiële) spread codes besproken in de context van codeertheorie, designtheorie en projectieve meetkunde. Zo zal de constructie van Beutelspacher van partiële spreads in een eindige projectieve ruimte leiden tot een interessante partiële spread code $\mathcal{C}_q(k, n; p, p')$. Hiervan zullen we de constructie en eigenschappen bespreken en dit zal ons leiden tot een decodeeralgoritme voor partiële spread codes. Daarnaast beschouwen we een ander voorbeeld van een partiële spread, die vanuit codeertheoretisch standpunt waarschijnlijk minder geschikt is, maar wiens grootte groter is dan de corresponderende partiële spread volgens de constructie van Beutelspacher. Hiervan zullen we, dankzij een computerzoektocht van Peter Vandendriessche, een meetkundige beschrijving geven van de bijhorende verzameling gaten.

Maar uiteraard is dit nog maar een begin. Er zijn nog steeds grenzen die verbeterd moeten worden, van vele klassieke concepten kunnen er nog q-analogons beschouwd worden en misschien vindt men andere constructies voor partiële spreads of nieuwe Steiner structuren... Ik hoop dat u door het lezen van dit werk de smaak te pakken heeft gekregen om over dit fascinerende onderwerp nog meer informatie te gaan vergaren en mogelijks zelfs hierover onderzoek naar te verrichten.

Door deze masterproef beschikbaar te maken voor het COST project, wil ik graag bijdragen tot een verdere ontwikkeling van *random network coding and designs over* $\mathbb{F}_q$.

Bibliography

[1] R. Ahlswede, L. Bäumer, N. Cai, H. Aydinian, V. Blinovsky, C. Deppe, and H. Mashurian. *General theory of information transfer and combinatorics*, volume 4123. Springer, 2007.

[2] R. Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.

[3] A. Beutelspacher. On t-covers in finite projective spaces. *Journal of Geometry*, 12(1):10–16, 1979.

[4] M. Braun, A. Kerber, and R. Laue. Systematic construction of q-analogs of t-(v, k, λ)-designs. *Designs, Codes and Cryptography*, 34(1):55–70, 2005.

[5] M. Braun and A. Wassermann. q-Steiner systems do exist. *arXiv preprint, arXiv:1211.2758*, 2012.

[6] A.E. Brouwer, A.M. Cohen, and A. Neumaier. Distance-regular graphs, A series of modern surveys in mathematics. *Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)*, 18(10), 1989.

[7] L. Chihara. On the zeros of the Askey-Wilson polynomials, with applications to coding theory. *SIAM Journal on Mathematical Analysis*, 18(1):191–207, 1987.

[8] C.J. Colbourn and R. Mathon. Steiner systems. *CRC Handbook of Combinatorial Designs*, page 66, 2010.

[9] COST. ICT COST Action IC1104. http://www.cost.eu/domains_actions/ict/Actions/IC1104, 2011.

[10] COST Action IC1104, Random Network Coding and Designs over GF(q). http://www.network-coding.eu, 2012.

[11] Universitat Autònoma de Barcelona. First European Training School in Network Coding. http://jornades.uab.cat/networkcodingts/content/vision, 2013.

[12] M. De Boeck and L. Storme. Theorems of Erdős-Ko-Rado type in geometrical settings. *Science China Mathematics,* submitted.

[13] P. Delsarte. An algebraic approach to association schemes of coding theory. *Philips Journal of Research*, 10:1–97, 1973.

[14] J. Eisfeld and L. Storme. Partial t-spreads and minimal t-covers in finite projective spaces. *Intensive Course on Finite Geometry and its Applications, Ghent University*, 2000.

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

[16] P. Erdős, C. Ko, and R. Rado. Intersection theorems for systems of finite sets. *The Quarterly Journal of Mathematics*, 12(1):313–320, 1961.

[17] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, 2011.

[18] T. Etzion and A. Vardy. On q-analogs of Steiner systems and covering designs. *Advances in Mathematics of Communications*, 5(2):161–176, 2011.

[19] T. Etzion and A. Vardy. Automorphisms of codes in the Grassmann Scheme. *arXiv preprint, arXiv:1210.5724*, 2012.

[20] P. Frankl and R.M. Wilson. The Erdős-Ko-Rado theorem for vector spaces. *Journal of Combinatorial Theory, Series A*, 43(2):228–236, 1986.

[21] E. Gorla and A. Ravagnani. Partial spreads in random network coding. *preprint*, 2012.

[22] R. Hill. *A first course in coding theory*. Oxford University Press, USA, 1990.

[23] J.W.P. Hirschfeld and J.A. Thas. *General Galois geometries*. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press Oxford, Oxford University Press, New York, 1991.

[24] T. Ho, M. Médard, R. Kötter, D.R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, 2006.

[25] H.D.L. Hollmann. A relation between Levenshtein-type distances and insertion-and-deletion correcting capabilities of codes. *IEEE Transactions on Information Theory*, 39(4):1424–1427, 1993.

[26] D.E. Knuth. Dancing links. *Millennial Perspectives in Computer Science: Proceedings of the 1999 Oxford-Microsoft Symposium in Honour of Sir Tony Hoare, J. Davies, B. Roscoe, J. Woodcock (Eds.), Palgrave*, pages 187–214, 2000.

[27] E.S. Kramer and D.M. Mesner. t-Designs on hypergraphs. *Discrete Mathematics*, 15(3):263–296, 1976.

[28] R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[29] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1994.

[30] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands, North-Holland, 1977.

[31] W.J. Martin and X.J. Zhu. Anticodes for the Grassmann and bilinear forms graphs. *Designs, Codes and Cryptography*, 6(1):73–79, 1995.

[32] C. Meyer. *Matrix analysis and applied linear algebra book and solutions manual*, volume 2. Society for Industrial and Applied Mathematics, 2000.

[33] S.E. Payne and J.A. Thas. *Finite generalized quadrangles*. Second Edition. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, 2009.

[34] M. Schwartz and T. Etzion. Codes and anticodes in the Grassman graph. *Journal of Combinatorial Theory. Series A*, 97(1):27–42, 2002.

[35] H. Tanaka. Classification of subsets with minimal width and dual width in Grassmann, bilinear forms and dual polar graphs. *Journal of Combinatorial Theory, Series A*, 113(5):903–910, 2006.

[36] L.M.G.M. Tolhuizen. The generalized Gilbert-Varshamov bound is implied by Turan's theorem [code construction]. *IEEE Transactions on Information Theory*, 43(5):1605–1606, 1997.

[37] A.-L. Trautmann. Finite spreads in random network coding. Slides of talk given at Colloquium on Galois Geometry, Ghent, May 4 2012, Ghent University, Belgium.

[38] A.-L. Trautmann. Constructions, decoding and automorphisms of subspace codes. *PhD, University of Zürich*, 2013.

[39] V. Verlé. Het lottoprobleem. *Master dissertation, Ghent University*, 1997.

[40] Wikipedia. http://en.wikipedia.org.

[41] R.M. Wilson. The exact bound in the Erdős-Ko-Rado theorem. *Combinatorica*, 4(2–3):247–257, 1984.

[42] S.-T. Xia and F.-W. Fu. Johnson type bounds on constant dimension codes. *Designs, Codes and Cryptography*, 50(2):163–172, 2009.