Des. Codes Cryptogr. (2016) 78:311–350
DOI 10.1007/s10623-015-0156-5

Galois geometries and coding theory

T. Etzion[1] · **L. Storme**[2]

Accepted: 12 October 2015 / Published online: 11 December 2015

Abstract Galois geometries and coding theory are two research areas which have been interacting with each other for many decades. From the early examples linking linear MDS codes with arcs in finite projective spaces, linear codes meeting the Griesmer bound with minihypers, covering radius with saturating sets, links have evolved to functional codes, generalized projective Reed–Muller codes, and even further to LDPC codes, random network codes, and distributed storage. This article reviews briefly the known links, and then focuses on new links and new directions. We present new results and open problems to stimulate the research on Galois geometries, coding theory, and on their continuously developing and increasing interactions.

Keywords Galois geometries · Coding theory · Network coding · Designs and codes over vector spaces

Mathematics Subject Classification 94B25 · 05B40 · 51E10

1 Introduction

Consider the projective space PG(N, q) of dimension N over the finite field $\mathbb{F}_q$ of order q. This is the projective space arising from the vector space $V(N+1, q)$ of dimension $N+1$ over

This is one of several papers published in *Designs, Codes and Cryptography* comprising the 25th Anniversary Issue.

✉ L. Storme
ls@cage.ugent.be
http://cage.ugent.be/∼ls

T. Etzion
etzion@cs.technion.ac.il
http://www.cs.technion.ac.il/∼etzion/

[1] Computer Science Department, Technion IIT, 32000 Haifa, Israel

[2] Department of Mathematics, Ghent University, Krijgslaan 281, 9000 Ghent, Belgium

the finite field $\mathbb{F}_q$ of order q, in which the $(i+1)$-dimensional vector subspaces are identified with the i-dimensional projective subspaces of $\mathrm{PG}(N,q)$. So the 1-dimensional subspaces of $V(N+1,q)$ correspond to the projective points of $\mathrm{PG}(N,q)$, the 2-dimensional subspaces to the projective lines of $\mathrm{PG}(N,q)$, ..., and the N-dimensional subspaces of $V(N+1,q)$ correspond to the $(N-1)$-dimensional projective subspaces of $\mathrm{PG}(N,q)$.

These $(N-1)$-dimensional subspaces of $\mathrm{PG}(N,q)$ are also called the *hyperplanes* of $\mathrm{PG}(N,q)$.

These finite projective spaces are also called *Galois geometries*, because they are defined over Galois fields.

This projective setting enables the use of many geometrical ideas and techniques. Besides being of great importance from a purely geometrical point of view, Galois geometries have been investigated because of their many links to other research areas, such as cryptography, design theory, graph theory, and coding theory.

Already in the seventies, a link between Galois geometries and coding theory is mentioned. In the first standard reference on coding theory of Sloane and MacWilliams [114], the authors explicitly mention the link between linear MDS codes and arcs in Galois geometries. The sentence in the chapter on linear MDS codes stating this chapter to be *one of the most fascinating in all of coding theory* has been cited by many researchers on Galois geometries to prove the relevance of their research domain.

These links then extended to other research problems, such as the linear codes meeting the Griesmer bound and covering radius of linear codes. These problems were investigated by using many different techniques, including geometrical techniques. Here, the geometrical equivalent substructures of minihypers and saturating sets were investigated in Galois geometries. But also functional codes and generalized projective Reed–Muller codes have been investigated via geometrical techniques.

More recently, new directions in coding theory appeared which intensified the close relationship between Galois geometries and coding theory. This includes LDPC codes, random network coding, and distributed storage.

This article wishes to draw attention to Galois geometries and coding theory, as two closely interacting research areas, by discussing a great variety of links between coding theory and Galois geometries.

We briefly recall known links between substructures in Galois geometries and coding theory which have appeared in the survey articles [90,109]. But, to stress the ongoing importance of these substructures in Galois geometries and their equivalent problems in coding theory, we focus on the important result of S. Ball, proving the MDS conjecture for linear MDS codes over prime fields, in order to keep motivating researchers to work on these known links and problems, and to show that there is still a lot of progress to be made.

This is then followed by recent results on functional codes and generalized projective Reed–Muller codes to give two other known domains linking Galois geometries and coding theory.

To highlight the new directions and to stress that the links between Galois geometries and coding theory are presently still greatly expanding, we focus on the newly established links between Galois geometries with random network coding and distributed storage. Here, many new relevant geometrical problems have arisen. These newly developed links increase the relevance of Galois geometries, and show that Galois geometries still have a great future.

To make this article self-contained, we first describe the following notations.

An $[n,k,d]$-*code* C over the finite field $\mathbb{F}_q$ of order q is a k-dimensional subspace of the vector space $V(n,q)$ of dimension n over the finite field of order q, having minimum distance d. A *generator matrix* of an $[n,k,d]$-*code* C is a $k \times n$ matrix G whose rows form

a basis for the code C. The *dual* code $C^{\perp}$ of an $[n, k, d]$-*code* C is the $[n, n-k, d^{\perp}]$-code consisting of all the vectors orthogonal to the codewords of C. A *parity check matrix* H for an $[n, k, d]$-*code* C is a generator matrix for its dual code $C^{\perp}$.

2 Early established links between Galois geometries and coding theory

2.1 Linear MDS codes and arcs in Galois geometries

This link starts from the well-known Singleton bound in coding theory.

Theorem 1 (The Singleton bound) *For a linear* $[n, k, d]$*-code* C, $d \leq n - k + 1$.

Definition 2 A linear $[n, k, n-k+1]$-code is called a linear *Maximum Distance Separable (MDS)* code.

The following theorem gives the fundamental properties of linear MDS codes, which will enable us to make the links to the geometrically equivalent arcs in Galois geometries.

Theorem 3 *Let* C *be a linear* $[n, k, d]$*-code, then the following properties are equivalent:*

(1) *The code* C *is a linear* $[n, k, n-k+1]$ *MDS code,*
(2) *every* k *columns of a generator matrix* G *of* C *are linearly independent,*
(3) *every* $n-k$ *columns of a parity check matrix* H *of* C *are linearly independent,*
(4) *the code* $C^{\perp}$ *is a linear* $[n, n-k, k+1]$ *MDS code.*

Independently, the following concept of arcs was defined in Galois geometries [89].

Definition 4 An *n-arc* in $\mathrm{PG}(k-1, q)$ is a set of n points, every k of which are linearly independent. An n-arc in $\mathrm{PG}(k-1, q)$ is called *complete* if and only if it is not contained in an $(n+1)$-arc of $\mathrm{PG}(k-1, q)$.

Definition 4 immediately makes the link with Theorem 3 (2), which gives the following equivalence.

Theorem 5 *The set* $K = \{g_1, \ldots, g_n\}$ *is an* n*-arc in* $\mathrm{PG}(k-1, q)$ *if and only if the* $k \times n$ *matrix* $G = (g_1 \cdots g_n)$ *defines a linear* $[n, k, n-k+1]$ *MDS code* C.

The equivalence between Theorems 3 (1) and 3 (4) now leads to the following geometrical result.

Theorem 6 *Let* $K = \{g_1, \ldots, g_n\}$ *be an* n*-arc in* $\mathrm{PG}(k-1, q)$ *defining the linear* $[n, k, n-k+1]$ *MDS code with generator matrix* $G = (g_1 \cdots g_n)$*, then there exists an* n*-arc* $\tilde{K} = \{h_1, \ldots, h_n\}$ *in* $\mathrm{PG}(n-k-1, q)$ *such that* $\tilde{K}$ *defines the dual* $[n, n-k, k+1]$ *MDS code* $C^{\perp}$ *via the parity check matrix* $H = (h_1 \cdots h_n)$ *of* C.

So the existence of an n-arc K in $\mathrm{PG}(k-1, q)$ implies the existence of an n-arc $\tilde{K}$ in $\mathrm{PG}(n-k-1, q)$. We say that an n-arc K in $\mathrm{PG}(k-1, q)$ and an n-arc $\tilde{K}$ in $\mathrm{PG}(n-k-1, q)$ are *C-dual* if and only if they define dual linear MDS codes.

The standard example of an n-arc in $\mathrm{PG}(k-1, q)$ is the normal rational curve.

Definition 7 A *normal rational curve* K in $\mathrm{PG}(k-1,q)$, $2 \leq k \leq q-1$, is a $(q+1)$-arc projectively equivalent to the set of points $\{(1,t,\ldots,t^{k-1}) | t \in \mathbb{F}_q^+\}$; $\mathbb{F}_q^+ = \mathbb{F}_q \cup \{\infty\}$, $\infty \notin \mathbb{F}_q$, $t = \infty$ defines the point $(0,\ldots,0,1)$.

In $\mathrm{PG}(2,q)$, a normal rational curve is called a *conic*, and in $\mathrm{PG}(3,q)$, a normal rational curve is called a *twisted cubic*.

The normal rational curves define the *Generalized Doubly-Extended Reed-Solomon (GDRS)* codes, i.e., the classical examples of linear MDS codes. These GDRS codes are used to encode music on compact discs [93] and are used in QR-codes [128].

The normal rational curve $K = \{(1,t,t^2) | t \in \mathbb{F}_q^+\}$ in $\mathrm{PG}(2,q)$, q even, i.e., a conic in $\mathrm{PG}(2,q)$, q even, can be extended by the point (0,1,0) to a $(q+2)$-arc, defining a $[q+2,3,q]$-code and a dual $[q+2,q-1,4]$-code.

The main conjecture regarding linear MDS codes states that the maximal length of a linear $[n,k,n-k+1]$-code over the finite field $\mathbb{F}_q$ of order q, $2 \leq k \leq q-1$, is equal to $q+1$, unless $k \in \{3, q-1\}$ and q is even.

The survey article [90] contains many tables on linear MDS codes and arcs in Galois geometries. We refer to these tables for the main results on the main conjecture regarding linear MDS codes, and also other results on linear MDS codes.

In this article, we wish to highlight the major breakthrough obtained by Ball [6]. The next theorem solved the MDS conjecture completely for linear MDS codes over prime fields. It is one of the best results in Galois geometries of the beginning of the 21st century.

Theorem 8 (Ball) [6] *The maximal length for a linear* $[n,k,n-k+1]$*-code over the finite field* $\mathbb{F}_q$ *of order* q*,* q *an odd prime,* $2 \leq k \leq q-1$*, is equal to* $q+1$*. If the length of the linear* $[n,k,n-k+1]$*-code over the finite field of order* q*,* q *an odd prime,* $2 \leq k \leq q-1$*, is equal to* $q+1$*, then the linear* $[n,k,n-k+1]$*-code is a GDRS code.*

This fundamental breakthrough was obtained by S. Ball by developing a *coordinate-free lemma of tangents* approach. Previous results, as enumerated in the tables of [90], made use of the lemma of tangents [89, Lemma 8.11].

The lemma of tangents was originally formulated for arcs in $\mathrm{PG}(2,q)$. It describes a relation between slopes of lines meeting the arc in one point.

Lemma 1 (Lemma of tangents) [89, Lemma 8.11] *For any* n*-arc* $\mathcal{K}$ *in* $\mathrm{PG}(2,q)$*, with* $3 \leq n \leq q+1$*, choose three of its points as the triangle of reference* $\mathbf{U}_0 = (1,0,0)$, $\mathbf{U}_1 = (0,1,0)$, $\mathbf{U}_2 = (0,0,1)$ *of the coordinate system.*

Let the following lines be the lines through $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2$*, only sharing one point with* $\mathcal{K}$*:*

$$X_1 - a_i X_2 = 0,\ X_2 - b_i X_0 = 0,\ X_0 - c_i X_1 = 0,\ i = 1,\ldots,t = q+2-n.$$

Then

$$\prod_{i=1}^{t} (a_i b_i c_i) = -1.$$

This relation enabled Segre to prove that a $(q+1)$-arc in $\mathrm{PG}(2,q)$, q odd, is always a conic. This result is stated in the next theorem, and is also known under the name: *The fundamental theorem of Galois geometries*, because it motivated many researchers to start studying problems in Galois geometries. Because it also is a characterization theorem on linear MDS codes, we also state the corresponding result in the language of coding theory.

Theorem 9 (Fundamental theorem of Galois geometries) [140] *In* PG$(2, q)$, *q odd, every* $(q+1)$*-arc consists of the point set of a conic.*

All the $[q+1, 3, q-1]$*-MDS codes and* $[q+1, q-2, 4]$*-MDS codes over the finite field* $\mathbb{F}_q$*, q odd, are GDRS codes.*

But the relative weakness lies in the fact that, in order to apply the lemma of tangents, each time three points of the arc are chosen as a basis for the projective plane PG$(2, q)$, and choosing a fixed basis is a rather hard restriction if the idea is to apply this lemma to several subsets of the arc.

But, S. Ball developed a coordinate free version of the lemma of tangents [89, Lemma 8.11] in the following way [6].

Assume that S is an arc of the projective space PG$(k-1, q)$, $k < q$. For any subset Y of $k-2$ elements of S, since there are at most $k-1$ points of S in a hyperplane of PG$(k-1, q)$, there are exactly $t = q+1-(|S|-k+2) = q+k-1-|S|$ hyperplanes containing Y and no other points of S.

Let ϕ_Y be a set of t pairwise linearly independent linear maps from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ with the property that, for each $\alpha \in \phi_Y$, $Ker(\alpha)$ is one of the t hyperplanes containing Y and no other point of S.

The *tangent function at Y* is defined, up to a scalar factor, as

$$T_Y(x) := \prod_{\alpha \in \phi_Y} \alpha(x),$$

and is a map from $\mathbb{F}_q^k$ to $\mathbb{F}_q$.

By working with this coordinate free version of the lemma of tangents, the results of Theorem 8 were obtained.

A further improvement to the result of Ball was obtained by Ball and De Beule.

Theorem 10 (Ball and De Beule) [7] *The maximal length for a linear* $[n, k, n-k+1]$*-code over the finite field* $\mathbb{F}_q$ *of order q,* $q = p^h$*, p prime,* $h > 1$*,* $2 \leq k \leq 2p-2$*, is equal to* $q+1$.

We refer to the articles [6,7] for the detailed description of this coordinate-free lemma of tangents approach. But we also wish to draw the attention to the following remark.

Remark 1 The lemma of tangents [89, Lemma 8.11] has been used to prove many results in Galois geometries.

It is very reasonable to state that this approach by S. Ball can be applied to other problems in Galois geometries. It is of great interest to study this new approach.

Therefore, as a research topic to work on, both in Galois geometries as in coding theory, we suggest to study this new technique developed by S. Ball, and to check results, both in Galois geometries and in coding theory, which used the original version of the lemma of tangents, to see whether it is possible to improve these results by applying the coordinate free version of the lemma of tangents.

Remark 2 There also exists a Singleton bound for nonlinear codes.

Since we will also need to discuss nonlinear codes in certain parts of this article, we introduce here the notation $(n, M, d)_q$ for a q-ary code C of length n, consisting of M codewords, and having minimum distance d.

For nonlinear codes, the Singleton bound is as follows.

Theorem 11 (Singleton bound for nonlinear codes) *Every* $(n, M, d)_q$*-code* C *satisfies* $M \leq q^{n-d+1}$.

An $(n, M, d)_q$*-code* C*, with* $M = q^{n-d+1}$*, is called a* MDS code.

2.2 Griesmer bound and minihypers

Let $\theta_{\lambda+1} = |\mathrm{PG}(\lambda, q)| = (q^{\lambda+1} - 1)/(q - 1)$.

We first define the geometrical concept of the minihypers in Galois geometries, and also present the Griesmer bound on linear codes to which specific classes of minihypers will be equivalent.

Definition 12 An $(f, m; N, q)$*-minihyper* (F, w) is a set of points F of the projective space $\mathrm{PG}(N, q)$, with a weight function w satisfying the conditions:

- $w : \mathrm{PG}(N, q) \to \mathbb{N} : P \mapsto w(P)$.
- $w(P) > 0 \Leftrightarrow P \in F$.
- $\sum_{P \in \mathrm{PG}(N,q)} w(P) = f$.
- $\min_{H \in \mathcal{H}} \left(\sum_{P \in H} w(P) \right) = m$, with $\mathcal{H}$ the set of all hyperplanes of $\mathrm{PG}(N, q)$.

In the literature on Galois geometries, such an $(f, m; N, q)$-minihyper (F, w) is also known under the name of *weighted m-fold blocking set of size f with respect to the hyperplanes of* $\mathrm{PG}(N, q)$.

Now we present the *Griesmer bound* for linear codes.

Theorem 13 (Griesmer bound) [83,146] *For every linear* $[n, k, d]$*-code over the finite field* $\mathbb{F}_q$ *of order q,*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = g_q(k, d).$$

Linear $[g_q(k, d), k, d]$-codes, i.e. meeting the Griesmer bound, are called *Griesmer codes*.

The link between minihypers in $\mathrm{PG}(k - 1, q)$ and linear $[n, k, d]$-codes over the finite field $\mathbb{F}_q$ meeting the Griesmer bound is described in the following way. This is based on Hamada and Helleseth [87].

For $(s - 1)q^{k-1} < d \leq sq^{k-1}$, d can be written uniquely as $d = sq^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$ such that:

(a) $0 \leq \lambda_1 \leq \cdots \leq \lambda_h < k - 1$,
(b) at most $q - 1$ of the values λ_i are equal to a given value.

Using this expression for d, the Griesmer bound for a linear $[n, k, d]$-code over the finite field $\mathbb{F}_q$ can be expressed as:

$$n \geq s\theta_k - \sum_{i=1}^{h} \theta_{\lambda_i+1}.$$

Hamada and Helleseth [87] showed that in the case $d = sq^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$, there is a one-to-one correspondence between the set of all non-equivalent $[n, k, d]$-codes over $\mathbb{F}_q$ meeting the Griesmer bound and the set of all projectively distinct $(\sum_{i=1}^{h} \theta_{\lambda_i+1}, \sum_{i=1}^{h} \theta_{\lambda_i}; k - 1, q)$-minihypers (F, w).

Belov et al. [12] gave a construction method for Griesmer codes, which is easily described by using the corresponding minihypers.

Consider in PG$(k-1,q)$ *a sum of* ϵ_0 *points,* ϵ_1 *lines,* ϵ_2 *planes,* ϵ_3 *solids, ...,* ϵ_{k-2} $(k-2)$*-dimensional subspaces, with* $0 \leq \epsilon_i \leq q-1, i = 0, \ldots, k-2$*, then such a sum defines a* $(\sum_{i=0}^{k-2} \epsilon_i \theta_{i+1}, \sum_{i=0}^{k-2} \epsilon_i \theta_i; k-1, q)$ *-minihyper* (F, w)*, where the weight of a point* R *of* PG$(k-1,q)$ *equals the number of objects, in the description above, in which it is contained.*

Now that the standard examples of minihypers are known, the characterization problem of minihypers, and equivalently of linear codes meeting the Griesmer bound, arises:

Characterize $(f, m; k-1, q)$*-minihypers* (F, w) *for given parameters* $f = \sum_{i=0}^{k-2} \epsilon_i \theta_{i+1}$, $m = \sum_{i=0}^{k-2} \epsilon_i \theta_i$, k*, and* q*.*

Fundamental research on this problem was performed by Hamada *et al* who, in many articles, obtained a lot of results on minihypers and who developed a great amount of techniques useful in the study of minihypers. Their main results are in [86,88].

Improvements to the results of [86,88] were found by, for instance, De Beule, Metsch, and Storme. We mention a concrete example of a characterization result on weighted minihypers. For other characterization results on minihypers, we refer to the survey article [109].

Theorem 14 (De Beule et al. [42]) *A* $(\sum_{i=0}^{k-2} \epsilon_i \theta_{i+1}, \sum_{i=0}^{k-2} \epsilon_i \theta_i; k-1, q)$*-minihyper, where* $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q}+1$*, is a sum of* ϵ_{k-2} *hyperplanes,* ϵ_{k-3} $(k-3)$*-dimensional spaces, ...,* ϵ_1 *lines, and* ϵ_0 *points, so it is of Belov-Logachev-Sandimirov type.*

Technique 15 The results on the minihypers are obtained via a variety of techniques. First of all, minihypers are particular examples of *blocking sets*. The blocking sets are an intensively investigated type of substructures in Galois geometries. They appear in many different research topics in Galois geometries [127]. Hence, characterization results on minimal blocking sets play a crucial role in the characterization of minihypers.

More precisely, there is the linearity conjecture on blocking sets and multiple blocking sets. Important information on blocking sets and t-fold blocking sets include 1 (mod p) results and t (mod p) results for small minimal 1-fold and small minimal t-fold blocking sets [23,72,151–153].

Proving this linearity conjecture will imply many new results on substructures in Galois geometries. This also includes many new possible results on minihypers, giving equivalent new results on linear codes meeting the Griesmer bound.

2.3 Covering radius and saturating sets

Definition 16 Let C be a linear $[n,k,d]$-code over the finite field $\mathbb{F}_q$ of order q. The *covering radius* of the code C is the smallest integer R such that every n-tuple in $\mathbb{F}_q^n$ lies at Hamming distance at most R from a codeword in C.

The following theorem will be the basis for making the link with the geometrically equivalent objects of the *saturating sets in Galois geometries*.

Theorem 17 *Let* C *be a linear* $[n,k,d]$*-code over the finite field* $\mathbb{F}_q$ *of order* q *with parity check matrix* $H = (h_1 \cdots h_n)$*.*

Then the covering radius of C *is the smallest integer* R *such that every* $(n-k)$*-tuple over* $\mathbb{F}_q$ *can be written as a linear combination of at most* R *columns of* H*.*

In Galois geometries, the following geometrical structure has been defined.

Definition 18 Let S be a subset of PG(N,q). The set S is called ρ*-saturating* when every point P from PG(N,q) can be written as a linear combination of at most $\rho+1$ points of S.

The preceding Theorem and Definition now lead to the following equivalence between saturating sets and covering radius of linear codes:

ρ-saturating sets S in $\mathrm{PG}(n-k-1,q)$ *determine the parity check matrices of linear* $[n,k,d]$*-codes with covering radius* $R=\rho+1$.

In the study of ρ-saturating sets, one of the most important research problems is the problem of finding ρ-saturating sets of the smallest possible cardinality. The cardinality of a smallest possible set S from $\mathrm{PG}(N,q)$ which is ρ-saturating is denoted by the parameter $k(N,q,\rho)$.

The survey article [109] presents a number of the known upper bounds on the parameter $k(N,q,\rho)$. We present two upper bounds because they were obtained by the construction of two nice examples of saturating sets [40,41].

Theorem 19 (1) *For* $q \geq 4$, $k(3,q,1) \leq 2q+1$.
(2) *For* $q \neq 3$, $k(5,q,2) \leq 3q+1$.

Technique 20 The 1-saturating sets and 2-saturating sets of Theorem 19 (1) and Theorem 19 (2) are defined by the columns of the following two matrices H_1 and H_2:

$$H_1 = \left[\begin{array}{ccc|c|ccccc} 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ a_1 & \cdots & a_q & 1 & 0 & 0 & \cdots & 0 \\ a_1^2 & \cdots & a_q^2 & 0 & 0 & 1 & \cdots & 1 \\ 0 & \cdots & 0 & 0 & 1 & a_2 & \cdots & a_q \end{array}\right]$$

and

$$H_2 = \left[\begin{array}{ccc|c|ccccc|ccccc|c} 1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ a_1 & \cdots & a_q & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ a_1^2 & \cdots & a_q^2 & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & a_2 & \cdots & a_q & a_1^2 & \cdots & a_q^2 & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_1 & \cdots & a_q & 1 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & 0 \end{array}\right],$$

with $\mathbb{F}_q = \{a_1 = 0, a_2, \ldots, a_q\}$.

These two particular examples show that by taking the unions of particularly selected subsets of Galois geometries, such as *lines* and *conics*, it is possible to obtain very good upper bounds on the parameter $k(N,q,\rho)$. In the matrix H_1, the first q columns are points of a conic and the last q columns are points of a line. In the matrix H_2, we recognize q points of two conics, and $q-1$ points of a line.

That is why we propose the search for particular subsets of points that are small saturating sets in Galois geometries as an interesting research problem. Also inductive arguments for the construction of small saturating sets of points are of great interest.

We refer to [36] and [77] for a standard reference on covering codes and for a survey making the link between covering codes and Galois geometries.

3 Functional codes and generalized projective Reed–Muller codes

We now turn to links between Galois geometries and coding theory, of a different nature.

We discuss functional codes and projective Reed–Muller codes. These are types of *evaluation codes*. Codewords arise by evaluating functions in either all the points of a projective space or on a particular, interesting, subset of the projective space.

We first concentrate on the projective Reed–Muller codes, and then on the functional codes.

3.1 Projective Reed–Muller codes

Recall $\theta_{n+1} = (q^{n+1} - 1)/(q - 1)$.

Consider the set $\mathcal{F}_d$ of the homogeneous polynomials of degree d over the finite field $\mathbb{F}_q$ in the variables $X_0, \ldots, X_n$. Consider also the n-dimensional projective space $\mathrm{PG}(n, q)$ over the finite field of order q, and order the points $P_0, \ldots, P_{\theta_{n+1}-1}$ of $\mathrm{PG}(n, q)$ in a certain way, where we normalize the coordinates of the points P_i by making the leftmost non-zero coordinate equal to one.

Then the *d-th order q-ary projective Reed–Muller code* $\mathrm{PRM}(q, d, n)$ is defined in the following way:

$$\mathrm{PRM}(q, d, n) = \{(f(P_0), \ldots, f(P_{\theta_{n+1}-1}))|f \in \mathcal{F}_d \cup \{0\}\}.$$

The length and dimension of the projective Reed–Muller code $\mathrm{PRM}(q, d, n)$ is known [107]. The minimum distance of these projective Reed–Muller codes has been studied in many papers.

Here, we wish to emphasize the following link between the minimum distance of the projective Reed–Muller codes and Galois geometries:

The non-zero codewords of minimum weight of $\mathrm{PRM}(q, d, n)$ *correspond to the algebraic hypersurfaces of degree d having the largest number of points in* $\mathrm{PG}(n, q)$.

By a result of Serre [141], for $d \leq q - 1$, it is known that they correspond to the algebraic hypersurfaces which are the union of d hyperplanes passing through a common $(n - 2)$-dimensional subspace of $\mathrm{PG}(n, q)$. Sørensen determined $d(\mathrm{PRM}(q, d, n))$ for $d \leq n(q - 1)$ [147].

Theorem 21 (1) (Serre [141]) *The minimum weight of the code $PRM(q, d, n)$, for $d \leq q-1$, is defined by the algebraic hypersurfaces of degree d which are the union of d hyperplanes, passing through a common subspace of dimension $n - 2$ of* $\mathrm{PG}(n, q)$.
So $d(PRM(q, d, n)) = q^n - (d - 1)q^{n-1}$ for $d < q$.

(2) (Sørensen [147]) *Let $d - 1 = r(q - 1) + s$, with $0 \leq s < q - 1$. For $d \leq n(q - 1)$, $d(PRM(q, d, n)) = (q - s)q^{n-r-1}$.*

A. Sboui determined the second and third weight of $\mathrm{PRM}(q, d, n)$, for some values of d [137, Corollary 4.3].

Theorem 22 (1) *The second weight of the code $PRM(q, d, N)$, $5 \leq d \leq \frac{q}{3} + 2$, is defined by the algebraic hypersurfaces $\mathcal{A}_2^d$ of degree d which are the union of d hyperplanes, $d - 1$ of which meet in a common subspace of dimension $N - 2$ and with the d-th hyperplane not passing through this common subspace of dimension $N - 2$.*

(2) *The third weight of the code $PRM(q, d, N)$, with $5 \leq d \leq \frac{q}{3} + 2$, is defined by the algebraic hypersurfaces $\mathcal{A}_3^d$ of degree d which are the union of d hyperplanes, $d - 2$ of which meet in a common subspace K_1 of dimension $N - 2$, and where the last two hyperplanes H_{d-1} and H_d meet in a subspace K_2, different from K_1, such that K_2 is contained in exactly one of the $d - 2$ hyperplanes passing through K_1.*

In [132], the authors proved that if $q > d(d - 1)/2$, then any algebraic hypersurface of degree d, not the union of d hyperplanes, contains fewer points than any algebraic hypersurface which is the union of d hyperplanes. The consequence of this result for the corresponding

code PRM(q, d, n) is as follows: the weight w_m^l given by the minimal hyperplane arrangement is the highest weight codeword in PRM(q, d, n) which can be given by any hyperplane arrangement. Moreover, for $q > d(d-1)/2$, any algebraic hypersurface of degree d containing an irreducible non-linear factor cannot correspond to a weight less than w_m^l.

The authors of [11] managed to extend this result by allowing also non-linear components in the results on the sizes of algebraic hypersurfaces. We state immediately the results in terms of the weights of the codewords of the d-th order q-ary projective Reed–Muller code PRM(q, d, n), and then afterwards give some information on how this result was obtained.

Theorem 23 (Bartoli et al. [11, Theorem 5.1]) *Let c be a non-zero codeword of the d-th order q-ary projective Reed–Muller code PRM(q, d, n), $d < \sqrt[3]{q}$, of weight*

(1)

$$w(c) < q^n - \left(\frac{r+d-4}{2}\right)q^{n-1} - ((d-r+1)^2 + d - 1 + 2\sqrt{q})q^{n-2} - (2d - r + 2\sqrt{q})q^{n-3} - \left(d - 1 + 2\sqrt{q}\right)\left(\frac{q^{n-3}-1}{q-1}\right),$$

when $d - r + 1$ is odd,

(2)

$$w(c) < q^n - \left(\frac{d+r-3}{2}\right)q^{n-1} - \left(\frac{(d-r+1)^2}{2} + d\right)q^{n-2} - \left(\frac{3d-r+1}{2}\right)q^{n-3} - d\left(\frac{q^{n-3}-1}{q-1}\right) + \frac{r+d}{2},$$

when $d - r + 1$ is even,

then c corresponds to an algebraic hypersurface of degree d in PG(n, q)*, containing at least r hyperplanes defined over $\mathbb{F}_q$.*

To obtain these results, the authors of [11] proceeded in the following way.

By using the Hasse-Weil bound [89, Sect. 2.9] on the number of points belonging to an absolutely irreducible algebraic curve of PG$(2, q)$, they determined upper bounds on the number of points of PG$(2, q)$ belonging to an algebraic curve of degree d in PG$(2, q)$ containing at most r lines of PG$(2, q)$.

Lemma 2 [11, Lemma 2.3] *Let C be an algebraic plane curve of degree d in* PG$(2, q)$*, such that $2 \le d \le \frac{\sqrt{q}}{2}$ and $q > 13$. If C contains at most r different lines defined over $\mathbb{F}_q$, then $|C| \le B_r$, where*

$$B_r = \begin{cases} \left(\frac{d+r}{2}\right)q + \frac{d-r}{2} + 1, d - r \text{ even}, \\ \left(\frac{d+r-1}{2}\right)q + 2\sqrt{q} + \frac{d-r+1}{2}, d - r \text{ odd}. \end{cases}$$

They then developed arguments to obtain similar upper bounds on the number of points belonging to an algebraic hypersurface Φ of degree d in PG(n, q) containing exactly $r - 1$ hyperplanes of PG(n, q), which led to the following theorem.

Theorem 24 (Bartoli et al. [11, Theorem 4.1]) *Let Φ be an algebraic hypersurface of degree $d < \sqrt[3]{q}$ in* PG(n, q)*, containing exactly $r - 1$ hyperplanes defined over $\mathbb{F}_q$, then*

(1)

$$|\Phi| \leq \left(\frac{r+d-2}{2}\right) q^{n-1} + ((d-r+1)^2 + d + 2\sqrt{q})q^{n-2} + (2\sqrt{q} + 2d - r + 1)q^{n-3} + \left(d + 2\sqrt{q}\right)\left(\frac{q^{n-3}-1}{q-1}\right),$$

when $d - r + 1$ *is odd,*

(2)

$$|\Phi| \leq \left(\frac{d+r-1}{2}\right) q^{n-1} + \left(\frac{(d-r+1)^2}{2} + d + 1\right) q^{n-2} + \left(\frac{3d-r+3}{2}\right) q^{n-3} + (d+1)\left(\frac{q^{n-3}-1}{q-1}\right) - \frac{r+d}{2},$$

when $d - r + 1$ *is even.*

Retranslating this result on the number of points on algebraic hypersurfaces of degree d led to the result in Theorem 23 on the small weight codewords of the d-th order q-ary projective Reed–Muller code $\mathrm{PRM}(q, d, n)$, $d < \sqrt[3]{q}$.

A more detailed use of algebraic geometry methods investigating the cardinality of algebraic hypersurfaces of degree d in $\mathrm{PG}(n, q)$, or a more detailed application of known results on the cardinality of algebraic hypersurfaces of degree d in $\mathrm{PG}(n, q)$, will make it possible to obtain more information on the weights of the codewords of the d-th order q-ary projective Reed–Muller code $\mathrm{PRM}(q, d, n)$.

Hence, as a research problem for this subsection, we propose to continue the investigation of the cardinality of algebraic hypersurfaces of degree d in $\mathrm{PG}(n, q)$, to improve bounds on this cardinality, and, equivalently, on the weights of the codewords of the d-th order q-ary projective Reed–Muller code $\mathrm{PRM}(q, d, n)$, and also to improve the knowledge on which algebraic hypersurfaces of degree d in $\mathrm{PG}(n, q)$ define which weights for the d-th order q-ary projective Reed–Muller code $\mathrm{PRM}(q, d, n)$.

3.2 Functional codes

Consider an algebraic variety $\mathcal{X}$ in $\mathrm{PG}(N, q)$. To define the functional codes in a correct way, denote the point set of $\mathcal{X}$ by $\{P_1, \ldots, P_n\}$, where the coordinates of the points P_i are normalized with respect to the leftmost non-zero coordinate. The functional code $C_h(\mathcal{X})$ is equal to

$$C_h(\mathcal{X}) = \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{F}_h\} \cup \{0\},$$

with $\mathcal{F}_h$ the set of the homogeneous polynomials of degree h over the finite field $\mathbb{F}_q$ of order q in the variables $X_0, \ldots, X_N$ [108].

Here, the idea is to construct a linear code by selecting a particular interesting algebraic variety $\mathcal{X}$ in $\mathrm{PG}(N, q)$, and also a particular degree h, to evaluate the points of this algebraic variety $\mathcal{X}$ in the homogeneous polynomials of degree h over the finite field $\mathbb{F}_q$ in the variables $X_0, \ldots, X_N$.

For instance, consider the set of all quadrics $\mathcal{Q}$ in $\mathrm{PG}(N, q)$ [91]. These are the sets of points satisfying homogeneous quadratic equations: $\mathcal{Q} : \sum_{0 \leq i \leq j \leq N} a_{ij} X_i X_j = 0$. Quadrics in $\mathrm{PG}(N, q)$ are either non-singular, or a cone over a non-singular quadric. The non-singular quadrics in $\mathrm{PG}(N, q)$ are:

- the non-singular parabolic quadric in PG(N, q), N even, having standard equation:

$$\mathcal{Q}(N, q) : X_0^2 + X_1X_2 + X_3X_4 + \cdots + X_{N-1}X_N = 0,$$

- the non-singular hyperbolic quadric in PG(N, q), N odd, having standard equation:

$$\mathcal{Q}^+(N, q) : X_0X_1 + X_2X_3 + \cdots + X_{N-1}X_N = 0,$$

- the non-singular elliptic quadric in PG(N, q), N odd, having standard equation:

$$\mathcal{Q}^-(N, q) : f(X_0, X_1) + X_2X_3 + \cdots + X_{N-1}X_N = 0,$$

with $f(X_0, X_1)$ a homogeneous quadratic equation over $\mathbb{F}_q$, irreducible over $\mathbb{F}_q$.

Consider a non-singular quadric $\mathcal{Q}$ of PG(N, q). Then the functional code $C_2(\mathcal{Q})$ is the linear code

$$C_2(\mathcal{Q}) = \{(f(P_1), \ldots, f(P_n))|f \in \mathcal{F}_2\} \cup \{0\},$$

defined over $\mathbb{F}_q$. The small weights of this functional code were investigated by Edoukou *et al* in [55].

The interesting geometrical results that were used in [55] are, first of all, that there is a classification of all types of, non-singular and singular, quadrics in Galois geometries, and, secondly, that two different quadrics define a pencil of quadrics. This led to, for instance, the following result.

Theorem 25 [55, Theorem 2.1] *Let $\mathcal{Q}$ and $\mathcal{Q}'$ be two quadrics in* PG(N, q) *with intersection equal to the set V.*

If $N \geq 6$ and

$$|V| > q^{N-2} + 2q^{N-3} + 2q^{N-4} + q^{N-5} + \cdots + q + 1,$$

then in the pencil of quadrics defined by the two quadrics $\mathcal{Q}$ and $\mathcal{Q}'$, there is a quadric equal to the union of two hyperplanes.

The preceding theorem implies that the smallest weights of the functional codes $C_2(\mathcal{Q})$, $\mathcal{Q}$ a non-singular quadric in PG(N, q), arise from the intersections of $\mathcal{Q}$ with the quadrics in PG(N, q) which are the union of two hyperplanes.

In [55], a detailed study was made of the intersections of a non-singular quadric in PG(N, q) with the union of two hyperplanes. This led to the determination of the five, and sometimes even six, smallest non-zero weights of the functional codes $C_2(\mathcal{Q})$, including the number of codewords with these weights. We refer to the tables of [55] for the exact data.

This research inspired the authors of [55] to investigate similar functional codes defined by Hermitian varieties in PG(N, q^2), because there is also a complete classification of all types of, non-singular and singular, Hermitian varieties. Let $\mathcal{F}$ be the $\mathbb{F}_q$-vector space of the zero polynomial and all homogeneous polynomials $(X_0, \ldots, X_N)A(X_0^q, \ldots, X_N^q)$ of degree $q + 1$ in $N + 1$ variables, with $A = (a_{ij}), 0 \leqslant i, j \leqslant N, a_{ij}^q = a_{ji}, a_{ij} \in \mathbb{F}_{q^2}$, defining Hermitian varieties of PG(N, q^2). In this part of the text, a Hermitian form will always denote a non-zero polynomial belonging to $\mathcal{F}$. For any Hermitian variety $\mathcal{H}$ of PG(N, q^2), the functional code $C_{Herm}(\mathcal{H})$ is the linear code

$$C_{Herm}(\mathcal{H}) = \{(f(P_1), \ldots, f(P_n))|f \in \mathcal{F}\},$$

defined over $\mathbb{F}_q$.

Let $\mathcal{H}$ be a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$ [91, Chapter 23]. In [54], the small weight codewords of the functional code $C_{Herm}(\mathcal{H})$ were characterized. Similarly as for the codes $C_2(\mathcal{Q})$, the following result was the basis for this characterization of the small weight codewords of the functional code $C_{Herm}(\mathcal{H})$.

Theorem 26 [54, Theorem 2.2] *Let $\mathcal{H}$ and $\mathcal{H}'$ be two Hermitian varieties in* $\mathrm{PG}(N, q^2)$ *with intersection equal to the set V.*

If $N \geq 6$ and

$$|V| > q^{2N-2} + 2q^{2N-4} + q^{2N-5} + q^{2N-6} + 2q^{2N-7} + 2q^{2N-9} + \cdots + 2q^3 + q,$$

then in the pencil of Hermitian varieties defined by the two Hermitian varieties $\mathcal{H}$ and $\mathcal{H}'$, there is a Hermitian variety equal to the union of $q+1$ hyperplanes passing through a common $(N-2)$-dimensional space.

The preceding theorem implies that the smallest weights of the functional codes $C_{Herm}(\mathcal{H})$, $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, arise from the intersections of $\mathcal{H}$ with the Hermitian varieties in $\mathrm{PG}(N, q^2)$ which are the union of $q+1$ hyperplanes.

In [54], this led to the determination of the four smallest non-zero weights of the functional codes $C_{Herm}(\mathcal{H})$, including the number of codewords with these weights. We refer to the tables of [54] for the exact data.

Shortly afterwards, more complicated functional codes were investigated.

For example, the functional codes $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$. The codewords of this code are defined by evaluating the points of $\mathcal{H}$ in the quadratic polynomials defined over $\mathbb{F}_{q^2}$.

The crucial elements in obtaining the results of [54] and [55] were the facts that two distinct quadrics define a pencil of quadrics and that two distinct Hermitian varieties define a pencil of Hermitian varieties. This fact is no longer true when considering a quadric in combination with a Hermitian variety. This meant that different arguments had to be used.

So, from now on, more elaborate geometrical arguments have to be used. In [10], the authors made a detailed investigation of intersections of quadrics with a non-singular Hermitian variety in the 4-dimensional projective space $\mathrm{PG}(4, q^2)$ to have these results in 4-dimensional projective space as the induction basis for their results on the intersections of quadrics with a non-singular Hermitian variety $\mathcal{H}$ in N-dimensional projective spaces $\mathrm{PG}(N, q^2)$, $N \geq 4$. We state the main result on this study of the intersections of quadrics with a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$ in the next theorem, where we use the following notation:

- $W_5 = q^7 + q^6 + 4q^5 - 2q^3 + 3q^2$,
- $W_6 = q^9 + q^8 + 4q^7 - 2q^5 + 2q^4$,
- $W_7 = q^{11} + q^{10} + 4q^9 - 2q^7 + 2q^6 + q^5 + 2q^4$,
- $W_N = q^{2N-3} + q^{2N-4} + 4q^{2N-5} - 2q^{2N-7} + 2q^{2N-8} + q^{2N-9} + \cdots + q^{N-2}$ if $N \geq 8$ is even,
- $W_N = q^{2N-3} + q^{2N-4} + 4q^{2N-5} - 2q^{2N-7} + 2q^{2N-8} + q^{2N-9} + \cdots + q^{N-2} + 2q^{N-3}$ if $N \geq 8$ is odd.

Theorem 27 [10, Theorem 3.3] *Let $\mathcal{H}$ be a fixed non-singular Hermitian variety in* $\mathrm{PG}(N, q^2)$.

Let Q be an arbitrary quadric in $\mathrm{PG}(N, q^2)$, $N \geq 4$. *If $|Q \cap \mathcal{H}| > W_N$, then Q is the union of two hyperplanes.*

The preceding result led to the determination of the five smallest non-zero weights of the functional codes $C_2(\mathcal{H})$, $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, $N \geq 4$. We refer to [85, Tables 3(a) and (b)] for the five smallest non-zero weights of $C_2(\mathcal{H})$, $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, $N \geq 4$. Note that by the improved arguments of [10], the condition $N < O(q^2)$ is not necessary anymore in these tables.

Since [10] first contained a detailed discussion of results on the intersections of arbitrary quadrics with a fixed non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, the authors also decided to investigate the functional codes $C_{Herm}(\mathcal{Q})$, with $\mathcal{Q}$ a fixed non-singular quadric in $\mathrm{PG}(N, q^2)$, in which the codewords are obtained by evaluating the points of $\mathcal{Q}$ in all the polynomials of $\mathcal{F}$ defining Hermitian forms of $\mathrm{PG}(N, q^2)$.

The discussion of the intersections of a given non-singular quadric with the Hermitian varieties again involved elaborate geometrical arguments. Here, it was again not possible to give the exact value for the minimum distance of the code $C_{Herm}(\mathcal{Q})$, with $\mathcal{Q}$ a non-singular quadric in $\mathrm{PG}(N, q^2)$. We summarize the results in the next theorem, where we rely on the following notation:

- $\overline{W}_N = q^7 + 2q^6 + 2q^5 - \frac{1}{2}q^4 - \frac{21}{4}q^3 + \frac{15}{8}q^2 + \frac{195}{16}q + 8$, $N = 5$ and $q > 2$,
- $\overline{W}_N = q^9 + q^8 + 3q^7 + 3q^6 - q^5 - 3q^4 - 4q^3 + 5q^2 + 16q + 16$, $N = 6$ and $q = 2$,
- $\overline{W}_N = W_N$ otherwise,

for $N \geq 5$.

Theorem 28 [10, Theorem 7.6] *Let $\mathcal{Q}$ be a non-singular quadric in* $\mathrm{PG}(N, q^2)$, $N \geq 5$, *and let H be an arbitrary Hermitian variety in* $\mathrm{PG}(N, q^2)$. *Then $|\mathcal{Q} \cap H| \leq \overline{W}_N$. Hence, the minimum distance of the code $C_{Herm}(\mathcal{Q})$ is at least $|\mathcal{Q}| - \overline{W}_N$.*

In [9], a next step was taken in the study of functional codes. The functional codes $C_h(\mathcal{Q})$, for $\mathcal{Q}$ a non-singular quadric in $\mathrm{PG}(N, q)$, small $h \geq 3$, $q > 9$, and for $N \geq 6$, were investigated.

So this means that a fixed non-singular quadric $\mathcal{Q}$ in $\mathrm{PG}(N, q)$ is intersected with algebraic hypersurfaces of degree h in $\mathrm{PG}(N, q)$.

The results of [9] prove that, for small h, the largest intersections of a non-singular quadric $\mathcal{Q}$ in $\mathrm{PG}(N, q)$, $N \geq 6, q > 9$, with the algebraic varieties of degree h are equal to the union of h quadric varieties of dimension $N - 2$. This means that this intersection is equal to the intersection of $\mathcal{Q}$ with an algebraic variety of degree h equal to the union of h hyperplanes. Even more information was obtained: the largest intersections arise from the intersection of $\mathcal{Q}$ with the union of h hyperplanes passing through a common $(N - 2)$-space.

The arguments that were used to obtain these results include Bézout's theorem on the intersection of algebraic hypersurfaces, results of Cafure and Matera [33] on the number of points on algebraic varieties, and particular properties of quadric varieties in finite projective spaces. To give an idea of the results of [9], we present the following corollary and theorem, which use the following notation, with $\sigma \in \mathbb{N}$:

$$B(\sigma) = \frac{\sigma q^{N-1} - (2h-1)(2h-2)q^{N-\frac{3}{2}} - (5(2h)^{\frac{13}{3}} + 4h^2)q^{N-2} - 1}{q-1};$$

$$T(\sigma) = \frac{\sigma q^{N-1} + (2h-1)(2h-2)q^{N-\frac{3}{2}} + (5(2h)^{\frac{13}{3}} + 4h^2)q^{N-2} - 1}{q-1}.$$

Corollary 29 [9, Corollary 1] *Let $\mathcal{X}$ be an algebraic hypersurface of degree $h \geq 3$ in* $\mathrm{PG}(N, q)$ *and $\mathcal{Q}$ a fixed non-singular quadric hypersurface in* $\mathrm{PG}(N, q)$, *not contained in $\mathcal{X}$. Suppose that $h < \sqrt{\frac{q}{8N}}$ and that*

Table 1 Minimum weights of the codes $C_h(\mathcal{Q})$, h small

$\mathcal{Q}(N,q)$, $N \geq 6$ even, $q > 9$	$q^{N-1} + (1-h)q^{N-2} - hq^{\frac{N-2}{2}}$
$\mathcal{Q}^+(N,q)$, $N \geq 7$ odd, $q > 9$	$q^{N-1} + (1-h)q^{N-2} - q^{\frac{N-1}{2}} + (h-1)q^{\frac{N-3}{2}}$
$\mathcal{Q}^-(N,q)$, $N \geq 7$ odd, $q > 9$	$q^{N-1} + (1-h)q^{N-2} - q^{\frac{N-1}{2}} - (h-1)q^{\frac{N-3}{2}}$

$$(2h)^{13/6} < \frac{\sqrt{q}}{4.35}.$$

Let $\mathcal{V} = \mathcal{X} \cap \mathcal{Q}$ and suppose that $|\mathcal{V}| \geq B(h)$, then $\mathcal{V}$ consists of h quadric varieties of dimension $N-2$ and $|\mathcal{V}| > T(h-1)$ also.

Theorem 30 [9, Theorem 4] *Let $\mathcal{V}$ be as in Corollary 29.*
Suppose $3 \leq h < \min\{\sqrt{\frac{q}{8N}}, \frac{1}{2}\left(\frac{q^{3/13}}{(4.35)^{6/13}}\right)\}$, $N \geq 6$, and $q > 9$. Let

$$M = \max_{\deg(\mathcal{X})=h, \mathcal{Q} \not\subseteq \mathcal{X}} |\mathcal{X} \cap \mathcal{Q}|.$$

If M is reached, then $\mathcal{X}$ consists of h hyperplanes intersecting in a common $(N-2)$-space.

These results led to the minimum weights for the functional codes $C_h(\mathcal{Q})$, h small mentioned in Table 1 [9, Table 3].

There are still several interesting types of functional codes, which should be investigated. The main focus in the preceding results was on functional codes related to quadrics and Hermitian varieties in Galois geometries. As a first problem, we suggest to improve the results on the functional codes presented in the preceding theorems, and as a second problem, we suggest to investigate functional codes defined by other types of varieties and substructures in Galois geometries.

4 Galois geometries and network coding

In this section, we will concentrate on the connections between the young research area of network coding and Galois geometries. We start in Sect. 4.1, where we present first the basic concepts and results on routing, explain the need for network coding, and discuss the great advantage of network coding on routing. MDS codes will play a major role in this comparison. The algebraic representation of the basic problems in network coding will be explained and the concept of random network coding will be presented. We will show that the advantage of random network coding on routing is not far from the related advantage of deterministic network coding. In our discussion, we will restrict ourselves to networks which are defined by directed acyclic graphs with unit capacities for all the edges.

In Sect. 4.2, metrics used for error-correction in network coding will be discussed. We will distinguish between coherent network coding and noncoherent network coding. One metric which is very important in the whole context of network coding is the rank-metric. This metric and its related codes will be considered in Sect. 4.3. In Sect. 4.4, we will discuss the class of subspace codes which are the first and the main connection between Galois geometries and random network coding. The codewords in a code from this class are subspaces of a vector space with dimension n over $\mathbb{F}_q$. As such they can be viewed as subspaces of the projective

geometry PG$(n-1, q)$. We continue in Sect. 4.5 where we discuss the most important family of codes for error-correction in network coding, the Grassmannian codes also known as constant dimension codes. They are called Grassmannian codes as they are subspaces of some Grassmannian $\mathcal{G}_q(n, k)$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$. In other words, the set of all $(k-1)$-subspaces of PG$(n-1, q)$. This family of codes is a subfamily of the subspace codes. Construction methods for such codes will be presented and methods from projective geometry can be applied to construct and to analyze codes from this family.

Related to Grassmannian codes are designs over $\mathbb{F}_q$ in a similar way that designs over sets are related to binary constant weight codes in the Hamming scheme. This topic, which is not new, has been re-motivated as a result of the new application of Grassmannian codes in random network coding. Designs over $\mathbb{F}_q$ are the q-analogs of designs over sets, where q-analog is an old concept. The concept of q-analog transfers problems and their solutions from a framework of sets to problems and their solutions in framework of vector spaces over $\mathbb{F}_q$. For q-analogs, a set becomes a subspace, the cardinality becomes the dimension, the union of sets becomes the sum of the related subspaces, i.e., the linear span of the related subspaces, and so on. Designs over $\mathbb{F}_q$, will be discussed in Sect. 4.6 and the q-analog of Steiner systems, i.e., q-Steiner systems will be considered in Sect. 4.7. They will be discussed with emphasis on the newly constructed q-analog of the Steiner system $S(2, 3, 13)$, and the intriguing unknown q-analog of the Steiner system $S(2, 3, 7)$. Spreads are q-analog of Steiner systems which are easy to obtain. They were heavily discussed in many connections on various aspects of Galois geometries. We will consider spreads and partial spreads in Sect. 4.8 from the point of view of Grassmannian codes. Another topic which was considered in Galois geometries in the context of spreads is parallelism. A parallelism is a partition of all subspaces of the same dimension from a given projective geometry into pairwise disjoint spreads. This problem and related ones will be discussed in Sect. 4.9, where we will show how codes in general and concepts used in network coding were of help in constructions of parallelisms. q-Steiner systems are also q-covering codes. Covering codes in the Grassmannian will be surveyed in Sect. 4.10. They are dual in one sense to the Grassmannian codes and in another sense they are dual to blocking sets in projective geometry. A very special and interesting family of codes in the Grassmannian is the family of equidistant codes. These codes will be considered in Sect. 4.11.

Finally, in Sect. 4.12, we will discuss another new topic in coding theory, namely, distributed storage codes. These codes are also related in some framework to a problem in network coding. We show a few connections between such codes for distributed storage and Galois geometries. During our survey and discussion, we will present the main open problems for future research in these topics.

Remark 3 In this section, topics will be discussed in the Grassmannian $\mathcal{G}_q(n, k)$ or in the projective space PG(n, q). In the Grassmannian $\mathcal{G}_q(n, k)$, vector dimensions are used, while in the projective space, projective dimensions are used. Here, a k-dimensional vector space $V(k, q)$ defines a $(k-1)$-dimensional projective space PG$(k-1, q)$.

To make the distinction between these two settings, in the Grassmannian setting of $\mathcal{G}_q(n, k)$, we will talk about *k-dimensional subspaces* $V(k, q)$ and in the projective space of *k-spaces* PG(k, q).

4.1 Routing versus network coding

The basic task of a network is to transfer objects (cars, fluids, data, depending on the application) from a set of sources to a set of sinks. This relatively old problem was considered

throughout the years and it is well known that the amount of information that can be transmitted in one round of communication is bounded by the min-cut/max-flow theorem [73]. The very basic algorithm to perform this task is known as the Ford–Fulkerson algorithm [73]. Network communication in the past referred to problems such as water flow in pipes, transportation networks, electricity distribution, etc., and the main research was to obtain better algorithms with improved complexity, to find shorter paths for transmission of the information, and to overcome faulty nodes. While effort was invested to achieve these goals, new challenges have been added twenty years ago when the internet came into life. The sources became transmitters and the sinks became receivers. New problems in transmitting the information arises, such as increasing the amount of information that can be transmitted to all the receivers. The bottleneck in this respect is the min-cut. While each receiver can receive the required information in the absence of other receivers, it is impossible that all receivers will obtain the information if the related paths from the transmitter are not (edge) disjoint. In 2000, Ahlswede, Cai et al. [1] introduced the novel idea of *network coding*. Like many fundamental concepts, it is rooted in a simple and beautiful basic idea. Traditionally, information flows in communication networks were treated just like fluid flows or cars on a highway network: each node in a network routes packets that it receives to its neighbors, while trying to avoid collisions of data streams as much as possible. However, unlike car + car=crash on a highway, $1 + 1 = 0$ in a binary field. Data packets are sequences of bits and several different packets can be coded into a single linear combination thereof. An assignment of a pre-determined linear combination of the source packets to each link (edge) in a network is known as a *network code*. The following toy example [1] illustrates this general idea. Consider the network in Fig. 1 below, known as the *butterfly*.

Suppose that each edge (link) has the capacity to transmit one packet error-free, and suppose we need to communicate the binary packets b_1 and b_2 from the source node S to both receiver nodes R_1 and R_2. It is easy to see that there is no way to do so using routing alone. However, simple coding (that is, adding the packets modulo 2) over the bottleneck edge (3,4) makes this possible.

In the framework which will be discussed in this section, a network is a finite graph $G = (V, E)$, where V is the set of vertices and E is the set of links (edges). We will only consider directed acyclic graphs in which each edge has a *capacity*, which is a positive integer. Non-integer capacities will not be considered in our discussion since the amount of data information is always represented by a nonnegative integer. Without loss of generality we assume that the capacity of each edge is one. This does not reduce the capability of the network since if larger integer capacity ℓ is needed for an edge, this edge can be replaced

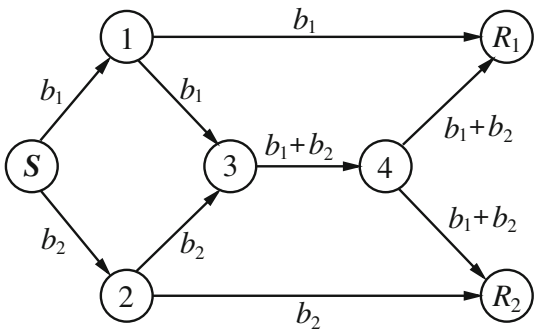

Fig. 1 The butterfly of Ahlswede, Cai, Li, and Yeung

with ℓ multiple parallel edges whose capacities are one. The network has k sources and N receivers. Each source has some inputs and each receiver has a list of demands which includes some of the inputs from some receivers. We start our exposition with the basic concepts and results related to routing. A *flow* is an assignment of zero/one values to the edges such that the total value of flow in the edges entering a vertex $v \in V$ is equal to the total value of flow in the edges leaving v. The *flow value* of the network is the net flow leaving the sources which is equal to the net flow entering the receivers. For a set of vertices $S \subset V$, the *cut* of S is the set of edges leaving S and entering $V \setminus S$. The capacity of the cut is the total sum of the capacities of its edges. When there exists exactly one source $s \in V$ and exactly one receiver $t \in V$, we require that for any cut S we have $s \in S$ and $t \in V \setminus S$. The following theorem is the celebrated min-cut/max-flow theorem [73].

Theorem 31 *Let $G = (V, E)$ be a directed acyclic graph with positive capacities on the edges. Let $s \in V$ be a vertex with no in-going edges (source) and $t \in V$ a vertex with no outgoing edges (receiver). Then, the maximum flow value from s to t in the network is equal to the minimum capacity in a cut of $S \subset V$ in the network, where $s \in S$ and $t \notin S$.*

Theorem 31 was formulated in terms of paths in the graph by Menger [116].

Theorem 32 *Let $G = (V, E)$ be a directed acyclic graph with positive capacities on the edges. Let $s \in V$ be a vertex with no in-going edges (source) and $t \in V$ a vertex with no outgoing edges (receiver). The maximum flow value from the source s to the receiver t is k if and only if there exists a maximum of k edge disjoint paths from s to t.*

We refer to the maximum flow value as the *rate* of the network and to the minimum capacity of a cut as the *capacity* $C_G(s, t)$ of the network. If we have one source s and a set $T \subset V$ of receivers, then the *capacity* of the network is defined as $C_G(s, T) = \min_{t \in T} C_G(s, t)$. If s is the unique source and all the other vertices of $V \setminus \{s\}$ are receivers, then instead of disjoint paths we should look for disjoint spanning trees rooted at s and this was formulated in Edmonds' theorem [53].

Theorem 33 *In a directed graph $G = (V, E)$, there are k edge disjoint spanning trees rooted at $r \in V$ if and only if $k \leq C_G(r, V \setminus \{r\})$.*

The proof of Theorem 33, given by Lovász [112], also provides a polynomial time algorithm to find the related disjoint spanning trees. But, for routing in the general case, only some of the vertices in V are receivers and instead of spanning trees we need another type of trees, called Steiner trees. For an undirected graph $G = (V, E)$ and a subset of vertices $T \subset V$, a *Steiner tree* is a tree, with the minimum number of edges, which contains all the vertices of T called *terminal vertices*, while the other vertices of the tree are called *Steiner vertices*. Finding such a tree is an NP-complete problem [101]. Let $G = (V, E)$ be a directed acyclic graph with a unique source $s \in V$ and a set of receivers $T \subset V \setminus \{s\}$. Assume furthermore that s has k inputs of unit value that it wants to transmit to all the receivers. Clearly, this can be done by using the network exactly once if there exist k edge disjoint trees rooted at s with exactly $|T|$ leaves which are the vertices of T. The number of such trees in a network is its *rate* and maximizing this rate is an NP-hard problem with reduction to the Steiner tree problem [100].

We now turn to network coding and surprisingly we will realize that network coding both increases the rate of some networks dramatically and also provides polynomial time algorithms to realize this rate. Consider first a network $G = (V, E)$ with k source nodes

$s_1, s_2, \ldots, s_k$ and a single receiver R. Each source has one packet to send to the receiver. We wish to know if the receiver can obtain the k packets when the network is applied exactly once. Consider the network $G' = (V', E')$, where $V' = V \cup \{\hat{s}\}$ and $E' = E \cup \{(\hat{s}, s_i) \mid 1 \leq i \leq k\}$, in which the unique source $\hat{s}$ has k packets. Clearly, the receiver R can obtain the k packets in G, when the network is applied exactly once, if and only if it can obtain the k packets in G', when the network is applied exactly once. Hence, by Theorem 32, the receiver in G' will obtain the k packets if and only if there exist k edge disjoint paths from $\hat{s}$ to R in G'. Equivalently, the receiver in G will obtain the k packets if there exist k edge disjoint paths from the k sources (one path from each source) to the receiver R. Now, suppose that instead of one receiver R, there are N receivers $r_1, r_2, \ldots, r_N$, and each one requires all the k packets. If the min-cut condition is satisfied for each receiver, without considering the other receivers, then we can send the information to the N receivers by using the network N times, one time for each receiver. One can easily construct networks where this is not possible when the network is applied exactly once. Moreover, it is not difficult to construct networks, where it is necessary to use the network N times or more precisely $\min\{k, N\}$ times if only routing is allowed. But, with network coding this task can be done by using the network exactly once. This is the multicast min-cut/max-flow theorem.

The idea behind network coding is very simple. Given a directed edge (u, v) in the network, when only routing is allowed this edge will only forward information from one of the in-coming edges of u. When network coding is allowed, the edge (u, v) will forward information which is a function of all (or some of) the information on the in-coming edges of u. A network is called *solvable* if we can encode the edges in such a way that each receiver R will be able to compute all the inputs by decoding the information on its in-coming edges. When only linear functions are used for encoding the information on the edges, an algebraic formulation was given to describe the transfer of information from the k sources (or equivalently the transfer of the k inputs from the unique source) to the N receivers. This algebraic formulation was described in detail in [104]. The vector of length k of the coefficients from the linear combination on an edge is called the *local coding vector*. Of course, the linear combinations on all the edges of paths which lead to a certain edge induce on this edge a linear combination of the original k inputs. The related k coefficients form the *global coding vector* for this edge. Assume again that the source has k inputs, each one is a packet (vector) of length n ($n = 1$ if the input is a scalar) over some finite field $\mathbb{F}_q$. The input is represented by a $k \times n$ matrix X (each row represents a packet of length n). Receiver r_j has a $k \times k$ *transfer matrix* A_j (computed with the algebraic formulation from the linear combinations on the paths from the source to r_j) for which $Y = A_j \cdot X$ is the output obtained at r_j. Receiver r_j also has the $k \times n$ output matrix Y. To recover the input X, the matrix A_j must be invertible. All the receivers can recover the inputs if all their related transfer matrices are nonsingular. This implies that the product of the determinants of all these transfer matrices is not zero. Since this determinant is a function of the coefficients in the linear combinations encoded on the edges, we can view this multiplication as a polynomial in the coefficients of the encoded edges. By the sparse zeroes lemma of Schwartz and Zippel [121], in a field $\mathbb{F}_q$, where q is greater than the total degree of the polynomial, there exists a substitution for these variables (the coefficients on the edges) such that the polynomial is not zero. By using this substitution, we will get a network coding solution for the network. A polynomial time algorithm to obtain a network code for the transfer of the information from the source to the receivers was presented in [99].

One of the interesting families of networks was defined in [131]. A network $N_{k,r,b}$ in this family has three layers, where all the edges are directed from the vertices in the first layer to vertices in the second layer, and from vertices in the second layer to vertices in the third layer.

In the first layer, the only vertex is the source node which has k inputs. In the second layer, there are r intermediate nodes. There is a link between the source and each one of these r nodes. The third layer has $\binom{r}{b}$ vertices, each one of them is a receiver. Each of these receivers has in-degree b and his in-coming edges are from a distinct subset of the $\binom{r}{b}$ subsets of vertices from the second layer. It was proved in [131] that the network $N_{k,r,b}$ is solvable if and only if there exists an $(r, q^k, r-b+1)_q$ code. Clearly, by the Singleton bound, a necessary condition that $N_{k,r,b}$ is solvable would be $k \leq b$. On the other hand, if $r \geq b$ and $q \geq r-1$ is a prime power, then there exists a linear $(r, q^b, r-b+1)_q$ MDS code and rate b is achievable on $N_{k,r,b}$. With this network we can also show the significant advantage of network coding over routing. It was proved in [99] that, for $N_{k,2k,b}$, rate k can be achieved with network coding using a $(2k, q^k, 2k-b+1)_q$ MDS code if $b \geq k$, while routing can achieve at most rate strictly less than two. This network can also be used to provide an example when a nonlinear network code is better than a linear network code [131] by using parameters where only nonlinear codes exist.

The next step is the concept of random network coding, which was presented in [92]. Instead of a fixed linear combination in each link, the linear combination is randomly chosen. An out-going edge of a vertex $v \in V$ will choose a random linear combination of the values on the in-coming edges of the vertex v. This linear combination is chosen over a very large finite field $\mathbb{F}_q$. The size q of the field is determined as a consequence of the following theorem [92].

Theorem 34 *Let G be a multicast solvable network with N receivers in which the coefficients for the linear combinations for the links are chosen independently and uniformly over $\mathbb{F}_q$. Let η be the total number of coefficients in the coding points of the network. Then the success probability that all the N receivers will obtain the information that was sent by the source node is at least $(1-\frac{N}{q})^\eta$, for $q > N$.*

We note that the total number of coefficients in the coding points is at most $n_c \cdot k$, where n_c is the number of coding points in the network.

The theory of network coding has expanded rapidly in the last fifteen years and now it is also connected to various other concepts and new research areas. It was no wonder that combinatorial designs in general and projective geometries in particular have found also some applications in these new research areas. The following subsections will reveal some of these connections and the research done on these topics.

4.2 Metrics in network coding

One of the most important aspects in network coding is how to handle errors since usually the channel on which the information is sent is not error-free. Errors can be caused by bad communication, insufficient capacity of the min-cut, by malicious actions, etc. There are mainly two different approaches to handle errors. The first one is to consider the messages as sequences and to apply the traditional error-correcting codes. A survey on error-correction for network coding in general and on such an approach in particular was given in [166]. This approach does not have strong connections to Galois geometries and hence it will not be discussed. We will devote our discussion to the second approach. To develop the theory of this approach, it will be enough to concentrate on the communication between one source and one receiver. Assume that the source sends a $k \times n$ matrix X (which represents k packets of length n). The receiver, who has a transfer matrix A, has received the output message $A \cdot X$. But, the matrix A does not provide all the necessary information due to channel insufficiency and up to ρ erasures could have occurred. In addition, an adversary has injected malicious

packets into the channel from an unknown set of t linearly independent vectors of length n, represented by a $t \times n$ matrix Z. These packets were sent and obtained by the receiver after a transfer matrix D was implemented on Z. Hence, the receiver will obtain the output $Y = A \cdot X + D \cdot Z$. This is the given scenario for which we continue with two types of models, coherent network coding and noncoherent network coding. In coherent network coding, the receiver knows the transfer matrix A and can use this fact for the error-correction procedure. In noncoherent network coding, this matrix is randomly chosen. In both cases, the transfer matrix D and the matrix Z are arbitrarily chosen by the adversary. It can be easily seen that when the matrix A is randomly chosen, the row span of the matrix X represents the inputs rather than the specific input vectors originated by the source. Therefore, the transmitted vectors will be considered as a subspace and this approach was taken in [105].

In this approach, the source sends a subspace V and an operator $\mathcal{H}_k$, called the "erasure operator", operates on the subspace V as follows. If the dimension of V is greater than k, then $\mathcal{H}_k(V)$ is a randomly chosen k-dimensional subspace of V. If the dimension of V is not greater than k, then $\mathcal{H}_k(V)$ is V. In addition to this erasure operator which can be caused by channel limitations and/or a malicious work done by the adversary, the adversary injects a few packets into the links of the channel. These packets form a t-dimensional subspace E, which is the error subspace. W.l.o.g. we can assume that the subspace $\mathcal{H}_k(V)$ and the subspace E should have a trivial intersection. Hence, the receiver will obtain the subspace $\mathcal{H}_k(V) \oplus E$. In order to perform error-correction in such a channel, a metric space and codes are defined as follows. Let $\mathcal{W}$ be an n-dimensional space over $\mathbb{F}_q$ and let $\mathcal{P}(\mathcal{W})$ be all its subspaces. $\mathcal{P}(\mathcal{W})$ is called the *projective geometry* or the *projective space* of $\mathcal{W}$. A code $\mathbb{C}$ in $\mathcal{P}(\mathcal{W})$ is a set of subspaces of $\mathcal{W}$ with a distance measure, the *subspace distance* d_S, defined on $\mathcal{P}(\mathcal{W})$ as follows. For two subspaces $U,\ V$ in $\mathcal{P}(\mathcal{W})$,

$$d_S(U, V) = \dim U + \dim V - 2\dim(U \cap V).$$

The *minimum distance*, $d_S(\mathbb{C})$, of a subspace code $\mathbb{C} \subseteq \mathcal{P}(\mathcal{W})$, is defined in the usual way as the smallest distance between any two distinct codewords of $\mathbb{C}$. Our goal in using the code $\mathbb{C}$ for error-correction in random network coding is that $\mathbb{C}$ will be able to correct errors and erasures if at most ρ erasures and at most t errors have occurred during the transmission until the receiver obtains its output. A minimum distance decoder will correct up to ρ erasures and t errors if the minimum subspace distance of the code $\mathbb{C}$ will be greater than $2(\rho + t)$. It is shown in [105] that a simple and a very effective way to produce subspace codes is to consider codes in which all subspaces have the same dimension. They have constructed codes which are based on linearized polynomials and are in fact the subspace version of Reed-Solomon codes. For simplicity and without loss of generality, we can assume that $\mathcal{W}$, the ambient space of dimension n, is in fact $\mathbb{F}_q^n$. The projective space $\mathcal{P}(\mathbb{F}_q^n)$, denoted in many papers by $\mathcal{P}_q(n)$, is in fact $\mathrm{PG}(n-1, q)$ and we will use only the projective geometry notation in the sequel. Equivalent codes to the ones obtained from linearized polynomials were constructed in [144] and they are based on rank-metric codes. These codes will be discussed in Sects. 4.3 and 4.5.

A novel approach to consider error-correction and metric spaces in general was considered and applied for network coding in [143]. The approach itself is beyond the scope of this paper, but the consequences are interesting (and can be obtained by the traditional error-correction approach). The output $Y = A \cdot X + D \cdot Z$, obtained by the receiver, is analyzed for the two models, the coherent network coding and the noncoherent network coding. For coherent network coding, where A is known to the receiver, while D and Z are random and chosen by the adversary, it was proved in [143] that the best strategy for error-correction is to consider X, Z and Y as matrices (and not as subspaces). The appropriate metric to consider is the rank-

metric distance between outputs and between the different matrices obtained by multiplying the matrix A by the various possible inputs.

For noncoherent network coding, it was proved in [143] that indeed, instead of considering the matrix X one should consider its row span, as was suggested in [105]. But, in contrary to [105], it was proved in [143] that the correct metric to consider in this case is the injection metric. For two subspaces U and V in PG$(n-1,q)$, the *injection distance* d_I is defined by

$$d_I(U,V) = \max\{\dim U, \dim V\} - \dim(U \cap V).$$

The minimum injection distance of a subspace code $\mathbb{C}$ is defined in the usual way. It was proved in [143] that a minimum distance decoder for the code $\mathbb{C}$ will correct any number of erasures up to ρ erasures and any number of errors up to t errors if and only if its minimum injection distance is greater than $\rho+2t$. This analysis proves that the injection metric and not the subspace metric is the correct distance measure for this case. Both metrics are equivalent when all subspaces of the code have the same dimension (which is the most important case). In other words, if the subspaces U and V have the same dimension then $d_S(U,V) = 2d_I(U,V)$. But, if the total number of erasures and errors together is bounded by τ, where τ is fixed, while ρ and t can vary and satisfy $\tau \geq \rho + t$, then the subspace distance will be the right distance measure and not the injection distance. This can be a reasonable scenario and hence the subspace distance should be also considered for random network coding and not only due to its theoretical interest.

In the following subsections, we will consider the various types of error-correcting codes which are mentioned in this section. Interesting families of such codes will be discussed and the emphasis will be on the codes connected to Galois geometries. Most of these codes are based on subspaces and the largest family of these codes is the one in which all the codewords have the same dimension. These codes are called constant dimension codes or Grassmannian codes since they are subsets from the Grassmann graph.

4.3 Rank-metric codes

As already mentioned, the rank-metric is used in coherent network coding for the purpose of error-correction. But, the importance of the rank-metric is beyond coherent network coding since many constructions of subspace codes are based on rank-metric codes, as will be explained in the sequel. Rank-metric codes are also connected to projective geometry since they can be viewed as one type of MDS codes.

For two $k \times \ell$ matrices A and B over $\mathbb{F}_q$, the *rank distance* is defined by

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

A $[k \times \ell, \varrho, \delta]$ *rank-metric code* $\mathcal{C}$ is a linear code whose codewords are $k \times \ell$ matrices over $\mathbb{F}_q$; they form a linear subspace with dimension ϱ of $\mathbb{F}_q^{k\times\ell}$, and for each two distinct codewords (matrices) A and B we have $d_R(A,B) \geq \delta$. For a $[k \times \ell, \varrho, \delta]$ rank-metric code $\mathcal{C}$, it was proved in [46,76,134] that

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

This bound, called the *Singleton bound for rank-metric codes*, is attained for all feasible parameters. Codes which attain this bound are called *maximum rank distance* codes (or MRD codes in short). Constructions for such codes are given in [46,76,134]. Assume w.l.o.g. that $k \geq \ell$, i.e., $\varrho \leq k(\ell-\delta+1)$. If the columns of the corresponding code are considered as elements of $\mathbb{F}_{q^k}$, then the code can be seen as an $[\ell, \varrho', \delta]$ code over $\mathbb{F}_{q^k}$, where $\varrho' = \frac{\varrho}{k} \leq$

$\ell - \delta + 1$. This is the Singleton bound, and hence the related MRD code is an MDS code when the columns are taken as elements from $\mathbb{F}_{q^k}$.

A $k \times \ell$ matrix A over $\mathbb{F}_q$ is *lifted* to the k-dimensional subspace of $\mathbb{F}_q^{k+\ell}$ whose generator matrix is $[I\ A]$. A $[k \times \ell, \varrho, \delta]$ *rank-metric code* $\mathcal{C}$ is *lifted* to a code $\mathbb{C}$ in $\mathcal{G}_q(k+\ell, k)$ by lifting all the codewords of $\mathcal{C}$, i.e., $\mathbb{C} = \{\langle [I\ A] \rangle \mid A \in \mathcal{C}\}$. This code $\mathbb{C}$ is a code in $\mathcal{G}_q(k+\ell, k)$ (i.e., $(k-1)$-subspaces in $\mathrm{PG}(k+\ell-1, q)$) with q^ϱ codewords and minimum subspace distance 2δ. If $\mathcal{C}$ is lifted to form a code $\mathbb{C}$, then $\mathbb{C}$ will be called a $(k+\ell, 2\delta, k)_q$ $\mathbb{C}^{\mathrm{MRD}}$ code or $\mathbb{C}^{\mathrm{MRD}}$ code in short. We will elaborate more on these codes in Sect. 4.5. How good is this simple construction? It appears that this construction yields asymptotically optimal codes (see Sect. 4.5).

One interesting property of the codes derived from lifting MRD codes is that a $\mathbb{C}^{\mathrm{MRD}}$ code can be resolved similarly to the set of lines in $\mathrm{PG}(n-1, q)$. It was proved that a $\mathbb{C}^{\mathrm{MRD}}$ code with minimum subspace distance 2δ can be partitioned into $\mathbb{C}^{\mathrm{MRD}}$ codes with minimum subspace distance $2\delta + 2$. This property, which will be discussed in Sect. 4.9, was observed in [66] in which it implied the following result.

Lemma 3 *A $\mathbb{C}^{MRD}$ code can be partitioned into $q^{(n-k)(k-\delta)}$ sets, called* parallel classes*, each one of size q^{n-k}, such that in each parallel class, each vector of $\mathbb{F}_q^n$ which does not start with k zeros is contained in exactly one codeword.*

Another class of rank-metric codes which are applied to construct larger subspace codes are the Ferrers diagram rank-metric codes [65]. This family is a generalization of the previous mentioned rank-metric codes and an upper bound on their sizes generalizes the related bound for rank-metric codes. There are a few constructions that attain this bound [65,81,163], but for most parameters no such construction is known. This question and its possible connections to Galois geometries is left for future research.

4.4 Subspace codes

An $(n, d)_q$ code is a subset of $\mathrm{PG}(n-1, q)$, such that the minimum distance in this subset of subspaces is d. As mentioned before, there are two possible distance measures for such codes which can be used in random network coding, the subspace distance and the injection distance, and the one chosen will be clear from the context. While the injection metric might be considered as a better measure for error-correction in random network coding, the subspace metric is more natural as it is the real q-analog of the Hamming metric for binary words. The injection metric is also a q-analog for another known distance metric for binary words, the asymmetric metric [59] (For two binary codewords u and v, let $Z(u, v)$ be the number of positions in which u has *ones* and v has *zeroes*. The *Hamming distance* is defined by $d_H(u, v) = Z(u, v) + Z(v, u)$, while the *asymmetric distance* is defined by $d_A(u, v) = \max\{Z(u, v), Z(v, u)\}$.). Both metrics (subspace and injection) coincide when all subspaces in the code have the same dimension and in this case the code is a Grassmannian code defined as follows. An $(n, 2\delta, k)_q$ code is a subset of $\mathcal{G}_q(n, k)$ with minimum subspace distance 2δ. Such codes will be considered in the next subsection. In this subsection, we will concentrate only on codes which are not of constant dimension. The three main construction methods for large subspace codes, with either the subspace distance or the injection distance, are the multilevel construction, puncturing of large codes as was presented in [65], and cyclic codes described in [68]. We will give a short description of the multilevel construction. For this, we need the following definition.

The *echelon Ferrers form*, $\mathrm{EF}(v)$, of a vector v of length n and weight k, is the $k \times n$ matrix in reduced row echelon form with leading entries (of rows) in the columns indexed

by the nonzero entries of v and "$\bullet$" in all entries which do not have terminal *zeroes* or *ones*. The dots of this matrix form the Ferrers diagram of EF(v). If we substitute elements of $\mathbb{F}_q$ in the dots of EF(v), we obtain a k-dimensional subspace X of $\mathcal{G}_q(n,k)$. Then, EF(v) will be also called the echelon Ferrers form of X.

We are now in a position to present the multilevel construction for codes in the projective space.

The multilevel construction

First step choose a binary code $\mathbf{C}$ of length n and minimum distance d. This code will be called the *skeleton code*. Let $\delta = 2d$ if the distance is the asymmetric distance and $\delta = 2\lceil \frac{d}{2} \rceil$ if the distance is the Hamming distance.

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

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

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

Fourth step lift $\mathcal{C}_{\mathcal{F}}$ to an $(n, 2\delta, k)_q$ code $\mathbb{C}_c$, for which the echelon Ferrers form of $X \in \mathbb{C}_c$ is EF(c).

Finally

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

Theorem 35 *The size of the code $\mathbb{C}$ is $\sum_{c \in \mathbf{C}} |\mathbb{C}_c|$ and it has minimum distance d.*

If we want to construct an $(n,d)_q$ code with the subspace distance, then $\mathbf{C}$, in the multilevel construction, should be a binary code with minimum Hamming distance d. If we want to construct an $(n,d)_q$ code with the injection distance, then $\mathbf{C}$, in the multilevel construction, should be a binary code with minimum asymmetric distance d. Grassmannian codes for this construction will be considered in the next subsection.

Lower bounds on the size of subspace codes are based on constructions, while upper bounds are based on analysis. Any $(n,d)_q$ code $\mathbb{C}$ in the projective space PG($n-1,q$) has a dimension distribution $D_0, D_1, \ldots, D_n$, where D_k is the number of codewords with dimension k in $\mathbb{C}$, i.e., $D_k = |\mathbb{C} \cap \mathcal{G}_q(n,k)|$. Then $\mathbb{C} \cap \mathcal{G}_q(n,k)$ is an $(n,d,k)_q$ code in $\mathcal{G}_q(n,k)$ and hence it is only natural that constructions of codes in the projective space can be based also on codes in the related Grassmannians, e.g. [65]. Similarly, upper bounds on the sizes of codes in the projective space are based on upper bounds on the sizes of codes in the related Grassmannian. Excellent examples are the linear programming bound, given in [68], and the semidefinite programming bound given in [3].

But, it should be noted that in spite of the above examples, connections between codes in the projective space PG($n-1,q$) and related problems in Galois geometries look to be weak and maybe less natural. It is of great interest to make stronger connections between these two areas to obtain new lower and upper bounds on the sizes of codes (either with the subspace distance or with the injection distance). But, with the lack of such results at this point of time, we will not discuss more bounds on the size of such codes, but will raise the problem of constructing codes and obtaining new upper bounds on the size of such codes by using tools from projective geometry.

4.5 Grassmannian codes

The family of Grassmannian codes is the most important one for error-correction in random network coding. It is also the most important family of codes related to projective geometry. A *Grassmannian code* is a subset of subspaces from $\mathcal{G}_q(n,k)$, i.e., $(k-1)$-subspaces of $\mathrm{PG}(n-1,q)$. As mentioned before, the injection metric and the subspace metric are equivalent in this case under the relation that for two k-subspaces X and Y we have that $d_S(X,Y) = 2d_I(X,Y)$.

A Grassmannian code is also called a *constant dimension code* since all the codewords have the same dimension. Let $\mathcal{A}_q(n,2\delta,k)$ denote the maximum size of an $(n,2\delta,k)_q$ code. Koetter and Kschischang [105], Etzion and Vardy [68] developed several upper bounds on $\mathcal{A}_q(n,2\delta,k)$. For a subspace code $\mathbb{C}$, we define the *orthogonal complement* $\mathbb{C}^\perp$ as the code which consists of all the dual subspaces of $\mathbb{C}$, i.e. $\mathbb{C}^\perp = \{X^\perp \mid X \in \mathbb{C}\}$. Since $d_S(X^\perp, Y^\perp) = d_S(X,Y)$ for any two subspaces $X, Y \in \mathbb{F}_q^n$, it follows that $\mathbb{C}$ and $\mathbb{C}^\perp$ have the same distance distribution and hence also the same minimum distance. Therefore, $\mathcal{A}_q(n,2\delta,k) = \mathcal{A}_q(n,2\delta,n-k)$ and hence only $(n,2\delta,k)_q$ codes and bounds on $\mathcal{A}_q(n,2\delta,k)$ for which $2k \le n$ will be considered in the sequel. The upper bounds on $\mathcal{A}_q(n,2\delta,k)$ are usually the q-analogs of the bounds on the related sizes of constant weight codes. These include the sphere packing bound and the Singleton bound [105], the Johnson bounds [67,68,164], from which the most important one was established earlier for linear authentication codes [162]:

Theorem 36

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

Theorem 36 can be iterated to obtain the iterated Johnson bound and the packing bound.

Theorem 37

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

As for lower bounds on $\mathcal{A}_q(n,2\delta,k)$, in [105], there is a construction of codes based on linearized polynomials, which yields the bound $\mathcal{A}_q(n,2\delta,k) \ge q^{(n-k)(k-\delta+1)}$. The same bound was developed in [144] by using lifted rank-metric codes (see Sect. 4.3). This bound was improved in [65] by using the multilevel construction. In this construction more codewords are added to a $\mathbb{C}^{\mathrm{MRD}}$ code. The skeleton code used in the multilevel construction to obtain an $(n,2\delta,k)_q$ code is a binary constant weight code with minimum Hamming distance 2δ. Usually, this construction will not yield optimal codes, but it is used to produce relatively large ones, and sometimes optimal ones (such as spread codes and partial spread codes which are defined in Sect. 4.8). In most cases, these are the largest known codes. An upper bound on the size of a code which contains $\mathbb{C}^{\mathrm{MRD}}$ code, for some selected parameters, can be found in [66]. More codes based on linearized polynomials were developed in [145]. The codes based on linearized polynomials, constructed in [105], are subcodes of these codes. But, the codes constructed in [145] are smaller in size than the related ones obtained by the multilevel construction. It was proved in [22] that for fixed q, k, and δ, the ratio between the upper bound of Theorem 37 and $\mathcal{A}_q(n,2\delta,k)$ tends to 1 as $n \to \infty$. But, the method used in [22] is based on probabilistic arguments and an explicit construction of the related codes is not known. A comparison between the upper bound given in Theorem 37 and the codes constructed by lifting and the ones obtained by the multilevel construction was given in [66].

Lemma 4

$$\frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} < \frac{q^{(n-k)(k-\delta+1)}}{\prod_{j=\delta}^{\infty}(1-q^{-j})}.$$

Define $Q_\delta(q) = \prod_{j=\delta}^{\infty}(1-q^{-j}), \delta \geq 1$. Since an $(n, 2\delta, k)_q$ $\mathbb{C}^{\mathrm{MRD}}$ code has $q^{(n-k)(k-\delta+1)}$ codewords, we have

Lemma 5 *The ratio between the size of an* $(n, 2\delta, k)_q$ $\mathbb{C}^{MRD}$ *code and the upper bound on* $\mathcal{A}_q(n, 2\delta, k)$ *given in Theorem 37 satisfies*

$$\frac{|\mathbb{C}^{MRD}|}{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q / \begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} > Q_\delta(q).$$

The function $Q_\delta(q)$ is increasing in q and also in δ. In Table 2, we provide several values of $Q_\delta(q)$ for different q and δ. For $q = 2$ these values were given in [14].

A lower bound on the ratio between the size of a constant dimension code generated by the multilevel construction, using $\delta = 2$ and part of a trivial constant weight code [66] and the upper bound on $\mathcal{A}_q(n, 2\delta, k)$ given in Theorem 37, is presented in Table 3. The values in the table are larger than the related values in the first row of Table 2 (note that in Table 3, $\delta = 2$ for all the entries; in Table 2, the entries are the same for all values of k.). Clearly, there are gaps between the lower and the upper bounds, but these are not dramatic.

Codes which admit a certain automorphism group are interesting in most metrics. Such codes were considered also in the Grassmannian. One such family of codes consists of the orbit codes [159,160] and another family contains the cyclic codes [68,106]. Cyclic codes have the potential to be very large ones (much larger than the ones obtained by the multilevel construction). Some major progress was achieved lately for the cyclic codes. In [78], a construction of codes which contain one degenerate orbit is given. In [13], a

Table 2 $Q_\delta(q)$

δ	q				
	2	3	4	5	7
2	0.5776	0.8402	0.9181	0.9504	0.9763
3	0.7701	0.9452	0.9793	0.9900	0.9966
4	0.8801	0.9816	0.9948	0.9980	0.9995
5	0.9388	0.9938	0.9987	0.9996	0.9999

Table 3 Lower bounds on ratio between Grassmannian codes obtained by the multilevel construction and the bound in Theorem 37 for $\delta = 2$

k	q				
	2	3	4	5	7
3	0.7101	0.8678	0.9267	0.9539	0.9771
4	0.6657	0.8571	0.9231	0.9524	0.9767
8	0.6274	0.8519	0.9219	0.9520	0.9767
30	0.6250	0.8518	0.9219	0.9520	0.9767

construction of cyclic codes based on subspace polynomials which are a subfamily of the linearized polynomials is given. In that paper, there is a construction for optimal codes which do not contain full length orbits. Finally, an optimal cyclic code in $\mathcal{G}_2(13,3)$ with minimum subspace distance 4 is given in [29]. The code admits two automorphisms, the Singer cycle and the Frobenius, which together form the normalizer of a Singer subgroup of GL(13,2). This code attains the bound of Theorem 37. Some automorphisms of Grassmannian codes were studied in [158]. Constructions for small dimensions might be attractive in this context. Interesting codes admitting some automorphisms were constructed in [27]. Some of these codes have an interesting combinatorial structure and some were found only by computer search. These were used to obtain lower bounds on $\mathcal{A}_2(n,4,3)$. Lower bounds on $\mathcal{A}_q(n,4,3)$ were also considered in [66]. Codes with subspaces of dimension 3 are of special interest mainly since the value of $\mathcal{A}_q(n,4,2)$ is known for all parameters. The value of $\mathcal{A}_q(n,4,3)$ is far from being solved for most parameters. One such value which was considered lately is $\mathcal{A}_q(6,4,3)$. It was proved that $\mathcal{A}_2(6,4,3)=77$ [96], while for $q>2$, $q^6+2q^2+2q+1\le\mathcal{A}_q(n,4,3)\le q^6+2q^3+1$ [39,96].

Another line of research for Grassmannian codes is based on the two geometric concepts of Schubert calculus and Plücker coordinates. These were considered in the connection of Grassmannian codes, for example in [64,133], and considering them for future research might also lead to new interesting results.

4.6 Designs over $\mathbb{F}_q$

Combinatorial designs in general and block designs in particular have many connections and applications to the theory of error-correcting codes, when the codewords are words of a given length over an alphabet of a given size. Galois geometries give classical, thoroughly studied, examples of designs by using the points and the subspaces, and these designs derived from projective geometries also yield interesting codes. If the codewords are subspaces of a vector space over $\mathbb{F}_q$, then we should consider the q-analog of designs and/or designs in the projective space. In this case, since the codewords are subspaces over $\mathbb{F}_q$, the codewords themselves are elements in the related Galois geometries.

It was suggested by Tits [156] in 1957 that combinatorics of sets could be regarded as the limiting case $q\to 1$ of combinatorics of vector spaces over the finite field $\mathbb{F}_q$. Indeed, there is a strong analogy between subsets of a set and subspaces of a vector space, expounded by numerous authors, see [37,79,161] and the references therein. In particular, the notions of t-designs have been extended to vector spaces by Cameron [34,35] and Delsarte [45] in the early 1970s. Specifically, let $\mathbb{F}_q^n$ be a vector space of dimension n over the finite field $\mathbb{F}_q$. A t-$(n,k,\lambda)_q$ design is a collection $\mathbb{B}$ of k-dimensional subspaces of $\mathbb{F}_q^n$, called *blocks*, such that each t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly λ blocks. If $\mathbb{B}$ contains all the k-dimensional subspaces of $\mathcal{G}_q(n,k)$, then the design is said to be *trivial*. Such t-designs over $\mathbb{F}_q$ are the q-analogs of conventional combinatorial designs.

The first examples of nontrivial t-designs over $\mathbb{F}_q$, with $t\ge 2$, were found by Thomas [154] in 1987. He has constructed 2-$(n,3,7)_2$ designs for $n\ge 7$, $n\equiv 1$ or 5 (mod 6). His construction was generalized by [148,150] to 2-$(n,3,q^2+q+1)_q$ designs for $n\ge 7$, $n\equiv 1$ or 5 (mod 6). In the first twenty years after the work of Thomas [154], until the seminal work of Koetter and Kschischang [105], several more constructions and designs were found [28,98,120]. Necessary conditions for the existence of such designs were given in [149].

The interest in network coding and the applications of codes over vector spaces have motivated new research on designs over $\mathbb{F}_q$. This research has been very productive and

has opened new directions for research. The intersection numbers of these designs were considered in [103]. Derived designs and residual designs were discussed in [102]. Some more results can be found in [26,122]. But, with no doubt, the strongest result was obtained recently in [71], where it was proved that t-$(n, k, \lambda)_q$ designs exist for all t and q, provided that $k > 12(t + 1)$ and n sufficiently large.

Recently, another type of q-analog for designs was considered. This is a large set of a t-$(n, k, \lambda)_q$ design. A *large set* of a design $\mathcal{S}$ is a partition of the space into disjoint copies of $\mathcal{S}$. Hence, a large set of t-$(n, k, \lambda)_q$ designs is a partition of $\mathcal{G}_q(n, k)$ into disjoint copies of t-$(n, k, \lambda)_q$ designs. Parallelism in projective geometry is a large set and this topic will be discussed separately in Sect. 4.9. Large sets for other designs were discussed in [30,31].

Another type of design over $\mathbb{F}_q$, which was defined recently, is the *subspace transversal design* [66]. This is not a direct q-analog of a transversal design as will be explained in the sequel, but it is related to Galois geometries.

Let $\mathbb{V}^{(n,k)}$ be the set of nonzero vectors of $\mathbb{F}_q^n$ whose first k entries form a nonzero vector. In other words, this set of vectors contains all vectors which are not contained in a specific $(n - k - 1)$-subspace $\hat{H}$ of $\mathrm{PG}(n - 1, q)$.

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

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

(1) $\mathbb{V}$ is a set of size $\frac{q^k-1}{q-1}q^{n-k}$ (the *points*). $\bigcup_{X\in\mathcal{G}_q(k,1)} \mathbb{V}_X^{(n,k)}$ is used as the set of points $\mathbb{V}$.
(2) $\mathbb{G}$ is a partition of $\mathbb{V}$ into $\frac{q^k-1}{q-1}$ classes of size q^{n-k} (the *groups*); the groups which are used are defined by $\mathbb{V}_X^{(n,k)}$, $X \in \mathcal{G}_q(k, 1)$.
(3) $\mathbb{B}$ is a collection of k-dimensional subspaces of $\mathbb{F}_q^n$ which contain nonzero vectors only from $\mathbb{V}^{(n,k)}$ (the *blocks*);
(4) each block meets each group in exactly one point;
(5) every t-dimensional subspace (with points from $\mathbb{V}$), which meets each group in at most one point, is contained in exactly one block.

This is not a direct q-analog of a transversal design since the elements of $\mathbb{V}_{\mathbf{0}}^{(n,k)}$ do not participate in any block of the design. It was proved in [66] that the codewords of an $(n, 2\delta, k)_q$ $\mathbb{C}^{\mathrm{MRD}}$ code form the blocks of a $\mathrm{STD}_q(k-\delta+1, k, n-k)$. It was also shown in [66] how to use the properties of a subspace transversal design to obtain better bounds on $\mathcal{A}_q(n, 2\delta, k)$ with codes which contain $\mathbb{C}^{\mathrm{MRD}}$ codes. These properties were also used to construct q-covering designs [61] and parallelisms [62], and they probably can be used for constructions of other related structures.

The amount of results on block designs over $\mathbb{F}_q$ is far below the enormous number of related results on block designs over sets. Except for the obvious question to form new designs with new parameters, there is always the question to find a q-analog for new types of block designs. How properties of Galois geometries are incorporated in such designs is another intriguing question.

4.7 q-Steiner systems

A *Steiner system* $S(t, k, n)$ is a collection S of k-subsets from an n-set $\mathcal{N}$ such that each t-subset of $\mathcal{N}$ is contained in exactly one element of S. Steiner systems were subject to extensive research in combinatorial designs [38]. A Steiner system is an optimal constant weight code in the Hamming scheme.

A *q-Steiner system*, the q-analog of a Steiner system, is a t-$(n, k, 1)_q$ *design*. In other words, a q-Steiner system $\mathbb{S}_q(t, k, n)$ is a collection $\mathbb{B}$ of k-dimensional subspaces from $\mathcal{G}_q(n, k)$ (called *blocks*) such that each t-dimensional subspace of $\mathcal{G}_q(n, t)$ is contained in exactly one block of $\mathbb{B}$. It is also a set $\mathbb{S}$ of $(k-1)$-subspaces of PG$(n-1, q)$ such that each $(t-1)$-subspace of PG$(n-1, q)$ is contained in exactly one subspace of $\mathbb{S}$. A q-Steiner system $\mathbb{S}_q(t, k, n)$ is also a constant dimension code which attains the bound of $\mathcal{A}_q(n, 2(k-t+1), k)$. As for other designs, q-Steiner systems are known to exist in the trivial cases $t = k$ or $k = n$, and in the case where $t = 1$ and k divides n. In the latter case, q-Steiner systems coincide with the classical notion of *spreads* in projective geometry and will be discussed in Sect. 4.8. Beutelspacher [17] asked in 1978 whether nontrivial q-Steiner systems with $t \geq 2$ exist, and this question has tantalized mathematicians ever since. The problem and its related consequences have been studied by numerous authors [2,32,69,117,139,154,155], without much progress towards constructing such q-Steiner systems. In particular, Thomas [155] showed in 1996 that certain kinds of $\mathbb{S}_2(2, 3, 7)$ q-Steiner systems (the smallest possible example) cannot exist. In 1999, Metsch [117] conjectured that nontrivial q-Steiner systems, with $t \geq 2$, do not exist in general. Furthermore, q-Steiner systems are diameter perfect codes in the Grassmann scheme. It was proved in [2] that these are the only diameter perfect codes in the Grassmann scheme.

Similarly to Steiner systems, simple necessary divisibility conditions for the existence of a given Steiner structure were developed in [139,149]. q-Steiner systems and Steiner systems are highly related. In [69,139], there are some constructions of Steiner systems derived from q-Steiner systems. Further research on q-Steiner systems seems to be fascinating, but also extremely difficult. Until recently, no q-Steiner system $\mathbb{S}_q(t, k, n), t > 1$, was known to exist. The following theorem, presented in [69], has given more indication that finding q-Steiner systems, with $t \geq 2$, would be a very difficult task.

Theorem 38 *If there exists a q-Steiner system $\mathbb{S}_2(2, k, n)$, then there exists a Steiner system $S(3, 2^k, 2^n)$.*

As a consequence of Theorem 38, if there exists a q-Steiner system $\mathbb{S}_2(2, 3, 7)$, then there exists a Steiner system $S(3, 8, 128)$. The existence of a Steiner system $S(3, 8, 128)$ is an open problem. This fact might give more evidence for the conjecture that a q-Steiner system $\mathbb{S}_2(2, 3, 7)$ does not exist.

Recently, the first nontrivial q-Steiner system $\mathbb{S}_q(t, k, n)$, with $t \geq 2$, was found. This is a q-Steiner system $\mathbb{S}_2(2, 3, 13)$ which has a large automorphism group [29]. It admits two automorphisms, the Singer cycle and the Frobenius, which together form the normalizer of a Singer subgroup of GL(13, 2). The q-Steiner system $\mathbb{S}_2(2, 3, 13)$ has this automorphism group and hence 15 representatives suffice to describe the whole system. The knowledge on q-Steiner systems is very small and there are many more research problems for future research. As we noted before, these problems are probably extremely difficult. We mention what we believe are the main three questions that we think are within reach, even though the task would be extremely difficult.

- Does there exist a q-Steiner system $\mathbb{S}_2(2, 3, 7)$? One technique to settle this problem was suggested in [63].

- Constructing new q-Steiner systems; systems of the form $\mathbb{S}_2(2, 3, p)$, $p \equiv 1 \pmod 6$ prime, might be the main target.
- Exclude the existence of any system for which the necessary divisibility conditions are satisfied.

4.8 Spreads and partial spreads

A *k-spread* in PG(n, q) is a set of trivially intersecting k-subspaces which contain all the points of PG(n, q). This implies that $q^{k+1} - 1$ divides $q^{n+1} - 1$ and hence $k + 1$ divides $n + 1$. A *partial k-spread* in PG(n, q) is a set of trivially intersecting k-subspaces. A partial $(k - 1)$-spread in PG$(n - 1, q)$ is an $(n, 2k, k)_q$ code and the number of subspaces in the largest such partial k-spread is the value of $\mathcal{A}_q(n, 2k, k)$. Hence, this value is of a special interest. A $(k - 1)$-spread in PG$(n - 1, q)$ is also a q-Steiner system $\mathbb{S}_q(1, k, n)$. Spreads and partial spreads are basic concepts which were very well studied in projective geometry. Some specific families of spreads, such as normal spreads [20,113], known also as geometric spreads, have also applications for coding in the Grassmannian, such as constructing small q-covering designs [61] or finding some of the asymptotic bounds for such designs [22] by using the results in [20]. The value of $\mathcal{A}_q(n, 2k, k)$, associated with the largest size of a partial $(k-1)$-spread in PG$(n-1, q)$, is of a very special interest since $(n, 2k, k)_q$ codes have applications as byte-correcting codes [60,95]. Decoding of such Grassmannian codes was considered in [82,115]. The known lower and upper bounds on $\mathcal{A}_q(n, 2k, k)$ are summarized in the following theorems. The first three well-known theorems can be found in [68].

Theorem 39 *If k divides n, then* $\mathcal{A}_q(n, 2k, k) = \frac{q^n-1}{q^k-1}$.

Theorem 40 $\mathcal{A}_q(n, 2k, k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor - 1$ *if* $n \not\equiv 0 \pmod k$.

Theorem 41 *Let* $n \equiv r \pmod k$. *Then, for all q,*

$$\mathcal{A}_q(n, 2k, k) \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1} .$$

We note that one method to obtain the lower bound of Theorem 41 is to apply the multilevel construction of codes presented in [66] (see Sect. 4.4). It is a major open problem to obtain more subspaces than the number derived from Theorem 41. Only one such family of codes is known (see Theorem 43). A general theorem on infinite families of such codes or a theorem on parameters in which this bound is tight would be a major breakthrough. The next theorem was proved in [95] for $q = 2$ and for any other q in [16].

Theorem 42 *If* $n \equiv 1 \pmod k$, *then* $\mathcal{A}_q(n, 2k, k) = \frac{q^n-q}{q^k-1} - q + 1 = \sum_{i=1}^{\frac{n-1}{k}-1} q^{ik+1} + 1$.

The value obtained in Theorem 42 is attained with an $(n, 2k, k)_q$ $\mathbb{C}^{\text{MRD}}$ code to which one subspace is added. By Theorems 39 and 42, the value of $\mathcal{A}_q(n, 4, 2)$ is known for all values of q and n. The value of $\mathcal{A}_2(n, 6, 3)$ is also known for $n \equiv 0$ or $1 \pmod 3$ from Theorems 39 and 42, and the last case $n \equiv 2 \pmod 3$ was proved in [58] as follows.

Theorem 43 *If* $n \equiv c \pmod 3$, *then* $\mathcal{A}_2(n, 6, 3) = \frac{2^n-2^c}{7} - c$.

The upper bound implied by Theorem 40 was improved for some cases in [52] in which a transformation of partial spreads into orthogonal arrays of strength two is considered.

Theorem 44 *If $n = k\ell + c$ with $0 < c < k$, then $\mathcal{A}_q(n, 2k, k) \leq \sum_{i=0}^{\ell-1} q^{ik+c} - \Omega - 1$, where $2\Omega = \sqrt{1 + 4q^k(q^k - q^c)} - (2q^k - 2q^c + 1)$.*

To summarize, the main open problem related to spreads and partial spreads is to improve the lower bound given in Theorem 41 or to show that this bound is actually tight.

4.9 Parallelism

A *k-parallelism* in PG(n, q) is a partition of the k-subspaces of PG(n, q) into pairwise disjoint k-spreads. Some parallelisms and related structures were obtained from various codes. Some 1-parallelisms of PG(n, q) were known for many years. For $q = 2$ and odd $n \geq 3$, there exists a 1-parallelism in PG$(n, 2)$, which was found in the context of the Preparata code and it is known that many such 1-parallelisms exist [4,5,165]. For any other power of a prime q, if $n = 2^i - 1$, $i \geq 2$, a 1-parallelism was given in [15]. Another family of 1-parallelisms in PG$(3, q)$, for $q \equiv 2 \pmod 3$, called *regular packings*, was constructed in [126]. In the last forty years, no new parameters for 1-parallelisms were shown until recently, when a 1-parallelism in PG$(5, 3)$ was proved to exist in [70]. A k-parallelism, for $k > 1$, was not known until a 2-parallelism in PG(5,2) was given in [135,136,157].

Two generalizations of the parallelism problem are defined as follows. The first one is to consider what is the maximum number of pairwise disjoint k-spreads that exist in PG(n, q)? Beutelspacher [19] proved that, if n is odd, then there exist $q^{2\lfloor \log n \rfloor} + \cdots + q + 1$ pairwise disjoint 1-spreads in PG(n, q). Based on MRD codes, it is proved in [62] that if $k + 1$ divides $n + 1$ and $n > k$, then there exist at least two disjoint k-spreads in PG(n, q) and there exist at least $2^{k+1} - 1$ pairwise disjoint k-spreads in PG$(n, 2)$.

For the second problem, we will define a *partial Grassmannian* $\mathcal{G}_q(n_1, n_2, k)$, $n_1 > n_2 \geq k$, as the set of all k-dimensional subspaces from the space $\mathbb{F}_q^{n_1}$ which are not contained in a given n_2-dimensional subspace U of $\mathbb{F}_q^{n_1}$. It can be readily verified that $\mathbb{V}^{(n,k)}$ (see Sect. 4.6) is a partial Grassmannian $\mathcal{G}_q(n, n - k, k)$, where $\mathbb{V}_0^{(n,k)}$ is the $(n - k)$-dimensional subspace U. A *spread* in $\mathcal{G}_q(n_1, n_2, k)$ is a set $\mathbb{S}$ of pairwise disjoint k-dimensional subspaces from $\mathcal{G}_q(n_1, n_2, k)$ such that each nonzero element of $\mathbb{F}_q^{n_1} \setminus U$ is contained in exactly one element of $\mathbb{S}$. A *parallelism* of $\mathcal{G}_q(n_1, n_2, k)$ is a set of pairwise disjoint spreads in $\mathcal{G}_q(n_1, n_2, k)$ such that each k-dimensional subspace of $\mathcal{G}_q(n_1, n_2, k)$ is contained in exactly one of the spreads. In other words, a parallelism in $\mathcal{G}_q(n_1, n_2, k)$ is a partition of all the $(k - 1)$-subspaces of PG$(n_1 - 1, q)$, which do not intersect nontrivially with a given $(n_2 - 1)$-subspace S of PG$(n_1 - 1, q)$, into partial $(k - 1)$-spreads such that each point of PG$(n_1 - 1, q)$, which is not contained in S, is contained in exactly one $(k - 1)$-subspace of each partial $(k - 1)$-spread. Beutelspacher [19] proved that if $k = 2$ then such a parallelism exists if $n_2 \geq 2, n_1 - n_2 = 2^i$, for all $i \geq 1$ and any $q > 2$. If $k = 2$ and $q = 2$ then such a parallelism exists if and only if $n_2 \geq 3$ and $n_1 - n_2$ is even. It was proved in [62] that if $k = n_1 - n_2$, then there exists a parallelism in $\mathcal{G}_q(n_1, n_2, k)$. This parallelism was obtained by considering the subspace transversal design defined in [66] which is based on an MRD code.

We end this subsection by presenting a parallelism of $\mathbb{C}^{\text{MRD}}$ codes which is used to prove some of the results mentioned in this subsection. The existence of this parallelism was proved in [66].

Lemma 6 *The codewords of an $(n, 2\delta, k)_q$ $\mathbb{C}^{MRD}$ code can be partitioned into $q^{(n-k)(k-\delta)}$ sets, called parallel classes, each one of size q^{n-k}, such that in each parallel class each element of $\mathbb{V}^{(n,k)}$ is contained in exactly one codeword.*

Corollary 1 *The codewords of an* $(n, 2\delta, k)_q$ $\mathbb{C}^{MRD}$ *code can be partitioned into* $q^{(n-k)(k-\delta)}$ *codes, each one of which is an* $(n, 2k, k)_q$ *code of size* q^{n-k}.

4.10 q-Covering designs

A Grassmannian code is a q-packing design. In combinatorics of sets, the dual definition for a packing design is a covering design. Hence, it is natural to consider also q-covering designs. A *q-covering design* $\mathbb{C}_q(n, k, r)$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n, k)$ such that each element of $\mathcal{G}_q(n, r)$ is contained in at least one element of $\mathbb{S}$. Let $\mathcal{C}_q(n, k, r)$ denote the minimum number of subspaces in a q-covering design $\mathbb{C}_q(n, k, r)$. In other words, a q-covering design $\mathbb{C}_q(n, k, r)$ is a collection $\mathbb{S}$ of $(k-1)$-subspaces of PG$(n-1, q)$ such that each $(r-1)$-subspace is incident with at least one element of $\mathbb{S}$. The concept of q-covering design was suggested first in [69] as a continuation for the coding approach in the Grassmannian space. But, this concept is highly related and in fact is dual in orthogonality of subspaces to blocking sets in projective geometry. A *blocking set* in PG(n, q) with respect to k-subspaces is a set of points meeting each k-subspace. This definition was generalized in [118]. A set $\mathbb{T}$ of t-subspaces in PG(n, q) such that each s-subspace, $t < s$, is incident with at least one element of $\mathbb{T}$ is called a *blocking set*. Hence, a blocking set is the q-analog of the well-known *Turán design* [43,44]. The complement of a *Turán design* is a covering design and similarly, the dual subspaces of a blocking set is a q-covering design. Even though the two problems are related, for a blocking set the two parameters $t < s$ are both fixed, while n is larger and usually much larger, while for the equivalent q-covering design $\mathbb{C}_q(n+1, n-t, n-s)$, $n-t > n-s$ are fixed, and n is larger, usually much larger. But, when n is small, the two problems are connected and results can be transferred between the two problems [61,69].

The first case for a blocking set, where $t = 0$, was completely considered and solved in [25]. The size of the smallest blocking set for $t = 1$ was considered in many papers, e.g. [56,118,119]. We note that blocking sets have also some different definitions (and maybe more popular definitions which define other structures which are not q-coverings). Blocking sets for the case $t = 1$ were considered also with respect to other properties related to Galois geometries. A recent survey of the known results on blocking sets is given in [24], where a large list of references concerning all aspects of blocking sets is given.

As in the case of error-correcting codes in the projective space (which are q-packing designs), there are some basic bounds on the size of a q-covering design. The first one is the q-analog of the Schönheim bound [138] which was given in [47,69] and is dual to the Johnson bound (see Theorem 36).

Theorem 45

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

In a similar way to the q-analog of the Johnson bound (Theorem 37), also the q-analog of the Schönheim bound can be iterated and a basic covering bound is obtained [69].

Theorem 46

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

where equality holds if and only if a q-Steiner system $\mathbb{S}_q(r, k, n)$ *exists.*

Similarly to Grassmannian codes, it was proved in [22] that for fixed q, k, and r, the ratio between the lower bound of Theorem 46 and $\mathcal{C}_q(n,k,r)$ tends to 1 as $n \to \infty$.

The next theorem is the basic theorem on blocking sets, and was given by Bose and Burton in [25].

Theorem 47 *If* $1 \leq r \leq n-1$, *then* $\mathcal{C}_q(n,n-1,r) = \frac{q^{r+1}-1}{q-1}$.

The following theorem was proved by Beutelspacher [18].

Theorem 48 *If* $1 \leq k \leq n$, *then* $\mathcal{C}_q(n,k,1) = \left\lceil \frac{q^n-1}{q^k-1} \right\rceil$.

Theorems 47 and 48 were proved again in the context of coverings by vector spaces in [69]. Several bounds on the size of blocking sets for s-subspaces by t-subspaces were given in [56,118] by considering sets of lines in the related projective geometry contained in r-subspaces. Lower bounds on the sizes of *Turán designs* given in [43,44] can be adopted to obtain lower bounds on the sizes of q-covering designs [69].

Upper bounds on $\mathcal{C}_q(n,k,r)$ are given by constructions. Most direct constructions are for small parameters and for larger parameters a recursive construction proved in [69] is used. This construction is the most basic upper bound on the size of a q-covering design.

Theorem 49 $\mathcal{C}_q(n,k,r) \leq q^{n-k}\mathcal{C}_q(n-1,k-1,r-1) + \mathcal{C}_q(n-1,k,r)$.

As mentioned before, the covering bound is attained asymptotically. Normal spreads [20,113], also known as geometric spreads [20], are used to prove the following values of $\mathcal{C}_q(n,k,r)$ [22].

Theorem 50 $\mathcal{C}_q(vm+\delta, vm-m+\delta, v-1) = \frac{q^{vm}-1}{q^m-1}$ *for all* $v \geq 2$, $m \geq 2$, *and* $\delta \geq 0$.

The next theorem given in [69] is used recursively once an exact bound for some given parameters is known.

Theorem 51

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

Theorem 51 implies a very interesting property on the behavior of optimal q-covering designs.

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

Similar to Grassmannian codes, the usage of $\mathbb{C}^{\mathrm{MRD}}$ codes as subspace transversal design made it possible to obtain some good bounds on $\mathcal{C}_2(n,k,2)$ and $\mathcal{C}_2(n,k,3)$, and these are given in [61]. These bounds are obtained by a direct construction. Finding new direct constructions to obtain small codes also for a larger field size is a problem for future research.

4.11 Equidistant codes

Equidistant codes are considered to be an interesting family of codes in the Hamming scheme with strong connections to combinatorial designs in general and projective geometry in particular. A code is called *equidistant* if the distance between any two distinct codewords is the same. In the Hamming scheme, it is well known that it is enough to consider constant

weight equidistant codes [75]. In this case, there is also a constant intersection between any two codewords. If the weight of a codeword is w and the constant intersection between codewords is t, then if the size of the code is greater than $(w-t)^2+(w-t)+1$, then the code is a *sunflower* (the intersection of size t is on the same t coordinates between any two codewords). If the size of the code is $(w-t)^2+(w-t)+1$, then such a code is known to exist if $t=1$, $w=q+1$, q a prime power, and it forms a projective plane of order q.

For an equidistant code in PG(n,q), any two distinct codewords (k-subspaces) have the same dimension of intersection. If the code has more than $\left(\frac{q^{k+1}-q^{t+1}}{q-1}\right)^2+\frac{q^{k+1}-q^{t+1}}{q-1}+1$ codewords, then the code is a *sunflower* (all the codewords intersect in the same t-subspace). This result and related ones which connect equidistant codes in the Hamming scheme and projective geometry are given in [48,49,74,84,97]. For example, the celebrated Erdős–Ko–Rado theorem determines the maximum size of a family in which the intersection size of two sets is at least t. The q-analog problem was considered for subspaces in [74,97]. Several simple constructions of related equidistant codes are given in [64]. These include spreads, partial spreads, dual codes, and the set of all k-subspaces of a given $(k+1)$-subspace in PG(n,q). A more sophisticated construction is based on the Plücker embedding [21]. The main result in [64] is given in the following theorem.

Theorem 52 *For every integer $n\geq 2$, there exists an equidistant code of $(n-1)$-subspaces in PG$(\binom{n+1}{2},q)$ of size $\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$.*

There are strong connections between equidistant codes in the projective geometry and equidistant rank-metric codes. Some of these connections can be readily verified from the discussion on lifting given in Sect. 4.5 and some other constructions can be found in [64].

The next theorem presents a dimension formula which ensures that when the codewords of an equidistant code generate a large dimension, then the code necessarily must be a sunflower.

Theorem 53 [8] *Let $C=\{\pi_1,\ldots,\pi_n\}$ be an equidistant code consisting of $(k-1)$-subspaces, pairwise intersecting in $(k-t-1)$-subspaces for some constant $t\geq 3$.*

If $\dim\langle\pi_1,\ldots,\pi_n\rangle\geq k+(t-1)(n-1)+1$, then C is a sunflower.

It is particularly interesting that the preceding bound is sharp. There exist besides the sunflower, two other types of equidistant codes $C=\{\pi_1,\ldots,\pi_n\}$ consisting of $(k-1)$-subspaces, pairwise intersecting in $(k-t-1)$-subspaces, $t\geq 3$, generating a space of exactly dimension equal to $k+(t-1)(n-1)$. We refer to [8] for the description of these two other types of equidistant codes.

4.12 Distributed storage codes

Network coding has been a very active research area in the last dozen of years and it has been expanded to various topics, some of which have started before the seminal work in [1,110]. As one example, where also projective geometry already has its role, we will briefly mention the fascinating area of distributed storage codes. Its strong connection to network coding was demonstrated in [50].

In a *distributed storage system (DSS)*, a file $x\in\mathbb{F}_q^B$ is stored in n storage *nodes*, α information symbols in each. The DSS is required to be resilient to node failures; i.e., it should be possible to retrieve the data from a lost node by contacting d other active nodes and downloading β information symbols from each one of them, an operation which is called *repair*. In addition, a *data collector* (DC) should be able to rebuild the stored file x by contacting any k active nodes, an operation which is called *reconstruction*. If the file is

coded with an ordinary error correcting code C prior to being stored in the system (usually by an MDS code), then C is called the *outer code*, and the DSS code is called the *inner code*.

A repair process that results in a new node which contains the exact same information as in the failed node is called an *exact repair*. A repair process which is not an exact repair is called a *functional repair*. Such a repair must maintain the system's ability of repair and reconstruction. The amount of data which is required for a repair is $d\beta$, and it is called the *repair bandwidth* of the code. Codes which minimize the repair bandwidth, i.e., $d\beta = \alpha$, are called *Minimum Bandwidth Regenerating (MBR) Codes*. Codes which minimize α, and thus have $\alpha = \frac{B}{k}$, are called *Minimum Storage Regenerating (MSR) Codes*. For more information on these topics the reader is referred to the seminal work [50] and to the short survey in [51].

Many other properties are important in the design of distributed storage codes. For example, locality of the symbols, i.e., repairing a failed node from a small number of nodes [80], is desirable. A *Self-Repairing Code (SRC)* is another type of code, which satisfies:

- repairs are possible without having to download an amount of data equivalent to the reconstruction of the original file x;
- the number of nodes required for repair depends only on how many nodes are missing and not on their identity.

Such codes based on spreads in projective geometry were designed in [124].

A framework to generate distributed storage codes based on subspaces was given in [94,123]. This framework combined with projective geometry was applied in [130] on the equidistant codes from [64] (which were mentioned before and are based on the Plücker embedding) to form codes which have good repairing, reconstruction, and locality properties. Other codes based on orbit codes were designed recently in [111]. Another family of codes for distributed storage, *fractional repetition codes*, was defined lately. In this family, exact repair is used, but no coding is required when a new node replaces a failed node, i.e., the nodes which participate in the repair have the exact parts of the failed nodes. The first such code was considered in [129] and related bounds were given in [57]. Codes which attain these bounds and improved bounds when such codes do not exist are given in [142], where the constructions are based on graphs, designs, and finite geometries. More constructions based on designs and finite geometries are given in [125].

The use of subspaces in Galois geometries for distributed storage codes is relatively new and provides new challenges for future research to those who are working in both areas.

Acknowledgments This research was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12.

References

1. Ahlswede E., Cai N., Li S.-Y.R., Yeung R.W.: Network information flow. IEEE Trans. Inf. Theory **46**, 1204–1216 (2000).
2. Ahlswede R., Aydinian H.K., Khachatrian L.H.: On perfect codes and related concepts. Des. Codes Cryptogr. **22**, 221–237 (2001).
3. Bachoc C., Passuello A., Vallentin F.: Bounds for projective codes from semidefinite programming. Adv. Math. Commun. **7**, 127–145 (2013).
4. Baker R.D.: Partitioning the planes $AG_{2m}(2)$ into 2-designs. Discret. Math. **15**, 205–211 (1976).
5. Baker R.D., van Lint J.H., Wilson R.M.: On the Preparata and Goethals codes. IEEE Trans. Inf. Theory **29**, 342–345 (1983).
6. Ball S.: On sets of vectors of a finite vector space in which every subset of basis size is a basis. J. Eur. Math. Soc. **14**, 733–748 (2012).

7. Ball S., De Beule J.: On sets of vectors of a finite vector space in which every subset of basis size is a basis II. Des. Codes Cryptogr. **65**, 5–14 (2012).
8. Barrolleta R.D., De Boeck M., Storme L., Suárez Canedo E., Vandendriessche P.: A bound for the sunflower property (preprint).
9. Bartoli D., Storme L.: On the functional codes arising from the intersections of algebraic varieties of small degree with a non-singular quadric. Adv. Math. Commun. **8**, 271–280 (2014).
10. Bartoli D., De Boeck M., Fanali S., Storme L.: On the functional codes defined by quadrics and Hermitian varieties. Des. Codes Cryptogr. **71**, 21–46 (2014).
11. Bartoli D., Sboui A., Storme L.: Bounds on the number of rational points of algebraic hypersurfaces over finite fields, with applications to projective Reed–Muller codes. Adv. Math. Commun. (to appear).
12. Belov B.I., Logachev V.N., Sandimirov V.P.: Construction of a class of linear binary codes achieving the Varshamov–Griesmer bound. Probl. Inf. Transm. **10**, 211–217 (1974).
13. Ben-Sasson E., Etzion T., Gabizon A., Raviv N.: Subspace Polynomials and Cyclic Subspace Codes. arXiv:1404.7739v2 (January 2015).
14. Berlekamp E.R.: The technology of error-correcting codes. Proc. IEEE **68**, 564–593 (1980).
15. Beutelspacher A.: On parallelisms in finite projective spaces. Geom. Dedicata **3**, 35–40 (1974).
16. Beutelspacher A.: Partial spreads in finite projective spaces and partial designs. Math. Z. **145**, 211–229 (1975).
17. Beutelspacher A.: Parallelismen in unendlichen projektiven Räumen endlicher Dimension. Geom. Dedicata **7**, 499–506 (1978).
18. Beutelspacher A.: On t-covers in finite projective spaces. J. Geom. **12**, 10–16 (1979).
19. Beutelspacher A.: Partial parallelisms in finite projective spaces. Geom. Dedicata **36**, 273–278 (1990).
20. Beutelspacher A., Ueberberg J.: A characteristic property of geometric t-spreads in finite projective spaces. Eur. J. Comb. **12**, 277–281 (1991).
21. Beutelspacher A., Rosenbaum U.: Projective Geometry: From Foundations to Applications. Cambridge University Press, Cambridge (1998).
22. Blackburn S., Etzion T.: The asymptotic behavior of Grassmannian codes. IEEE Trans. Inf. Theory **58**, 6605–6609 (2012).
23. Blokhuis A., Lovász L., Storme L., Szőnyi T.: On multiple blocking sets in Galois planes. Adv. Geom. **7**, 39–53 (2007).
24. Blokhuis A., Sziklai P., Szőnyi T.: Blocking sets in projective spaces. In: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry, pp. 61–84. Nova Academic Publishers, New York (2011).
25. Bose R.C., Burton R.C.: A characterization of flat spaces in finite geometry and the uniqueness of the Hamming and the MacDonald codes. J. Comb. Theory **1**, 96–104 (1966).
26. Braun M.: New 3-designs over the binary field. Int. Electron. J. Geom. **6**, 79–87 (2013).
27. Braun M., Reichelt J.: q-Analog of packing designs. J. Comb. Des. **22**, 306–321 (2014).
28. Braun M., Kerber A., Laue R.: Systematic construction of q-analogs of $t-(v, k, \lambda)$-designs. Des. Codes Cryptogr. **34**, 55–70 (2005).
29. Braun M., Etzion T., Östergård P.R.J., Vardy A., Wassermann A.: Existence of q-Analogs of Steiner Systems. arXiv:1304.1462 (April 2013).
30. Braun M., Kiermaier M., Kohnert A., Laue R.: Large sets of subspace designs. arXiv:1411.7181 (November 2014).
31. Braun M., Kohnert A., Östergård P.R.J., Wassermann A.: Large sets of t-designs over finite fields. J. Comb. Theory Ser. A **124**, 195–202 (2014).
32. Braun M., Kiermaier M., Nakić A.: On the Automorphism Group of the Binary q-Analog of the Fano Plane. arXiv:1501.07790 (January 2015).
33. Cafure A., Matera G.: Improved explicit estimates on the number of solutions of equations over a finite field. Finite Fields Appl. **12**, 155–185 (2006).
34. Cameron P.: Generalisation of Fisher's inequality to fields with more than one element. In: McDonough T.P., Mavron V.C. (eds.) Combinatorics. London Mathematical Society Lecture Note Series, vol. 13, pp. 9–13. Cambridge University Press, Cambridge (1974).
35. Cameron P.: Locally symmetric designs. Geom. Dedicata **3**, 65–76 (1974).
36. Cohen G., Honkala I., Litysn S., Lobstein A.: Covering Codes. North-Holland Mathematical Library 54, North-Holland, Amsterdam (1997).
37. Cohn H.: Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients. Am. Math. Mon. **111**, 487–495 (2004).
38. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs. Chapman and Hall/CRC Press, Boca Raton, FL (2007).
39. Cossidente A., Pavese F.: On subspace codes. Des. Codes Cryptogr. doi:10.1007/s10623-014-0018-6.

40. Davydov A.A.: Constructions and families of covering codes and saturated sets of points in projective geometry. IEEE Trans. Inf. Theory **41**, 2071–2080 (1995).
41. Davydov A.A., Östergård P.R.J.: On saturating sets in small projective geometries. Eur. J. Comb. **21**, 563–570 (2000).
42. De Beule J., Metsch K., Storme L.: Characterization results on arbitrary weighted minihypers and on linear codes meeting the Griesmer bound. Adv. Math. Commun. **2**, 261–272 (2008).
43. De Caen D.: Extension of a theorem of Moon and Moser on complete subgraphs. Ars Comb. **16**, 5–10 (1983).
44. De Caen D.: The current status of Turán's problem on hypergraphs. In: Frankl, P., Füredi, Z., Katona, G., Miklós, D. (eds.) Extremal Problems for Finite Sets, pp. 187–197. János Bolyai Mathematical Society, Budapest (1994)
45. Delsarte P.: Association schemes and t-designs in regular semilattices. J. Comb. Theory Ser. A **20**, 230–243 (1976).
46. Delsarte P.: Bilinear forms over a finite field, with applications to coding theory. J. Comb. Theory Ser. A **25**, 226–241 (1978).
47. Dentice E.F., Zanella C.: Bose–Burton type theorems for finite Grassmannians. Discret. Math. **309**, 363–370 (2009).
48. Deza M.: Une propriété extrémale des plans projectifs finis dans une classe de codes equidistants. Discret. Math. **6**, 343–352 (1973).
49. Deza M., Frankl P.: Every large set of equidistant $(0, +1, -1)$-vectors forms a sunflower. Combinatorica **1**, 225–231 (1981).
50. Dimakis A., Godfrey P., Wu Y., Wainwright M., Ramchandran K.: Network coding for distributed storage systems. IEEE Trans. Inf. Theory **56**, 4539–4551 (2010).
51. Dimakis A., Ramchandran K., Wu Y., Suh C.: A survey on network codes for distributed storage. Proc. IEEE **99**, 476–489 (2011).
52. Drake D.A., Freeman J.W.: Partial t-spreads and group constructible (s, r, μ)-nets. J. Geom. **13**, 210–216 (1979).
53. Edmonds J.: Edge-disjoint branchings. In: Rustin R. (ed.) Combinatorial Algorithms, pp. 91–96. Algorithmics Press, New York (1972).
54. Edoukou F.A.B., Hallez A., Rodier F., Storme L.: On the small weight codewords of the functional codes $C_{herm}(X)$, X a non-singular Hermitian variety. Des. Codes Cryptogr. **56**, 219–233 (2010).
55. Edoukou F.A.B., Hallez A., Rodier F., Storme L.: A study of intersections of quadrics having applications on the small weight codewords of the functional codes $C_2(Q)$, Q a non-singular quadric. J. Pure Appl. Algebra **214**, 1729–1739 (2010).
56. Eisfeld J., Metsch K.: Blocking s-dimensional subspaces by lines in PG$(2s, q)$. Combinatorica **17**, 151–162 (1997).
57. El Rouayheb S., Ramchandran K.: Fractional repetition codes for repair in distributed storage systems. In: 48-th Annual Allerton Conference on Communications, Control and Computing, pp. 1510–1517 (2010).
58. El-Zanati S., Jordon H., Seelinger G., Sissokho P., Spence L.: The maximum size of a maximal 3-spread in a finite vector space over GF(2). Des. Codes Cryptogr. **54**, 101–107 (2010).
59. Etzion T.: New lower bounds for asymmetric and unidirectional codes. IEEE Trans. Inf. Theory **37**, 1696–1704 (1991).
60. Etzion T.: Perfect byte-correcting codes. IEEE Trans. Inf. Theory **44**, 3140–3146 (1998).
61. Etzion T.: Covering of subspaces by subspaces. Des. Codes Cryptogr. **72**, 405–421 (2014).
62. Etzion T.: Partial k-Parallelisms in finite projective spaces. J. Comb. Des. **23**, 101–114 (2015).
63. Etzion T.: A New Approach to Examine q-Steiner Systems. arXiv:1507.08503 (July 2015).
64. Etzion T., Raviv N.: Equidistant codes in the Grassmannian. Discret. Appl. Math. **186**, 87–97 (2015).
65. Etzion T., Silberstein N.: Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams. IEEE Trans. Inf. Theory **55**, 2909–2919 (2009).
66. Etzion T., Silberstein N.: Codes and designs related to lifted MRD codes. IEEE Trans. Inf. Theory **59**, 1004–1017 (2013).
67. Etzion T., Vardy A.: Error-correcting codes in projective spaces. In: International Symposium on Information Theory, pp. 871–875 (2008).
68. Etzion T., Vardy A.: Error-correcting codes in projective spaces. IEEE Trans. Inf. Theory **57**, 1165–1173 (2011).
69. Etzion T., Vardy A.: On q-analogs for Steiner systems and covering designs. Adv. Math. Commun. **5**, 161–176 (2011).
70. Etzion T., Vardy A.: Automorphisms of codes in the Grassmann scheme. arXiv:1210.5724 (October 2012).

71. Fazeli A., Lovett S., Vardy A.: Nontrivial t-designs over finite fields exist for all t. J. Comb. Theory Ser. A **127**, 149–160 (2014).
72. Ferret S., Storme L., Sziklai P., Weiner Zs.: A t (mod p) result on weighted multiple $(n-k)$-blocking sets in PG(n, q). Innov. Incid. Geom. **6/7**, 169–188 (2007/2008).
73. Ford Jr. L.R., Fulkerson D.R.: Maximal flow through a network. Can. J. Math. **8**, 399–404 (1956).
74. Frankl P., Wilson R.M.: The Erdős–Ko–Rado theorem for vector spaces. J. Comb. Theory Ser. A **43**, 228–236 (1986).
75. Fu F., Kløve T., Luo Y., Wei V.K.: On equidistant constant weight codes. Discret. Applied Math. **128**, 157–164 (2003)
76. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**, 1–12 (1985).
77. Giulietti M.: The geometry of covering codes: small complete caps and saturating sets in Galois spaces. In: Surveys in Combinatorics 2013. London Mathematical Society Lecture Note Series, vol. 409, pp. 51–90. Cambridge University Press, Cambridge (2013).
78. Gluesing-Luerssen H., Morrison K., Troha C.: Cyclic orbit codes and stabilizer subfield. Adv. Math. Commun. **9**, 177–197 (2015).
79. Goldman J.R., Rota G.-C.: On the foundations of combinatorial theory IV: finite vector spaces and Eulerian generating functions. Stud. Appl. Math. **49**, 239–258 (1970).
80. Gopalan P., Hauang C., Simitci H., Yekhanin S.: On the locality of codeword symbols. IEEE Trans. Inf. Theory **58**, 6925–6934 (2012).
81. Gorla E., Ravagnani A.: Subspace Codes from Ferrers Diagram. arXiv:1405.2736 (May 2014).
82. Gorla E., Manganiello F., Rosenthal J.: An algebraic approach for decoding spread codes. Adv. Math. Commun. **6**, 443–466 (2012).
83. Griesmer J.H.: A bound for error-correcting codes. IBM J. Res. Dev. **4**, 532–542 (1960).
84. Hall J.I.: Bounds for equidistant codes and partial projective planes. Discret. Math. **17**, 85–94 (1977).
85. Hallez A., Storme L.: Functional codes arising from quadric intersections with Hermitian varieties. Finite Fields Appl. **16**, 27–35 (2010).
86. Hamada N., Helleseth T.: A characterization of some q-ary codes $(q > (h-1)^2, h \geq 3)$ meeting the Griesmer bound. Math. Jpn. **38**, 925–940 (1993).
87. Hamada N., Helleseth T.: Codes and minihypers. Optimal codes and related topics. In: Proceedings of the EuroWorkshop on Optimal Codes and Related Topics, Sunny Beach, Bulgaria, 10–16 June, pp. 79–84 (2001).
88. Hamada N., Maekawa T.: A characterization of some q-ary codes $(q > (h-1)^2, h \geq 3)$ meeting the Griesmer bound: part 2. Math. Jpn. **46**, 241–252 (1997).
89. Hirschfeld J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Clarendon Press, Oxford (1998).
90. Hirschfeld J.W.P., Storme L.: The packing problem in statistics, coding theory and finite projective spaces: update 2001. Developments in Mathematics. In: Blokhuis A., Hirschfeld J.W.P., Jungnickel D., Thas J.A. (eds.) Proceedings of the Fourth Isle of Thorns Conference on Finite Geometries, Chelwood Gate, 16–21 July, vol. 3, pp. 201–246. Kluwer Academic Publishers, Dordrecht (2000).
91. Hirschfeld J.W.P., Thas J.A.: General Galois geometries. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York (1991).
92. Ho T., Médard M., Koetter R., Karger D.R., Effros M., Shi J., Leong B.: A random linear network coding approach to multicast. IEEE Trans. Inf. Theory **52**, 4413–4430 (2006).
93. Hoffman D.G., Leonard D.A., Lindner C.C., Phelps K.T., Rodger C.A., Wall J.R.: Coding Theory: The Essentials. Marcel Dekker, New York (1992).
94. Hollmann H.: Storage codes; coding rate and repair locality. In: International Conference on Computing, Networking and Communications (ICNC), pp. 830–834 (2013).
95. Hong S.J., Patel A.M.: A general class of maximal codes for computer applications. IEEE Trans. Comput. **21**, 1322–1331 (1972).
96. Honold T., Kiermaier M., Kurz S.: Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4. Contemp. Math. **632**, 157–176 (2015).
97. Hsieh W.N.: Intersection theorems for systems of finite vector spaces. Discret. Math. **12**, 1–16 (1975).
98. Itoh T.: A new family of 2-designs over GF(q) admitting SL$_m(q^\ell)$. Geom. Dedicata **69**, 261–286 (1998).
99. Jaggi S., Sanders P., Chou P.A., Effros M., Egner S., Jain K., Tolhuizen L.M.G.M.: Polynomial time algorithms for multicast network code construction. IEEE Trans. Inf. Theory **51**, 1973–1982 (2005).
100. Jain K., Mahdian M., Salavatipour M.R.: Packing Steiner trees. In: Proceedings of the SODA 2003, Baltimore MD, pp. 266–274 (2003).
101. Karp R.: Reducibility among combinatorial problems. In: Miller R.E., Thatcher J.W. (eds.) Complexity and Computer Computations, pp. 85–104. Plenum Press, New York (1972).
102. Kiermaier M., Laue R.: Derived and residual subspace designs. Adv. Math. Commun. **9**, 105–115 (2015).

103. Kiermaier M., Pavčević M.O.: Intersection numbers for subspace designs. J. Comb. Des. **23**, 463–480 (2015).
104. Koetter R., Médrad M.: An algebraic approach to network coding. IEEE Trans. Netw. **11**, 782–795 (2003).
105. Koetter R., Kschischang F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory **54**, 3579–3591 (2008).
106. Kohnert A., Kurz S.: Construction of large constant dimension codes with a prescribed minimum distance. In: Lecture Notes Computer Science, vol. 5393, pp. 31–42 (2008).
107. Lachaud G.: The parameters of projective Reed–Muller codes. Discret. Math. **81**, 217–221 (1990).
108. Lachaud G.: Number of points of plane sections and linear codes defined on algebraic varieties. In: Arithmetic, Geometry, and Coding Theory. (Luminy, France, 1993), pp. 77–104. Walter De Gruyter, Berlin (1996).
109. Landjev I., Storme L.: Galois geometries and coding theory. In: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry, pp. 187–214. NOVA Academic Publishers, New York (2012).
110. Li S.-Y.R., Yeung R.W., Cai N.: Linear network coding. IEEE Trans. Inf. Theory **49**, 371–381 (2003).
111. Liu S., Oggier F.: On the design of orbit storage codes. In: 4th International Castle Meeting on Coding Theory and Applications, Palmela, Spain (2014).
112. Lovász L.: On two minimax theorems in graph theory. J. Comb. Theory Ser. B **21**, 96–103 (1976).
113. Lunardon G.: Normal spreads. Geom. Dedicata **75**, 245–261 (1999).
114. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).
115. Manganiello F., Gorla E., Rosenthal J.: Spread codes and spread decoding in network coding. In: International Symposium on Information Theory, pp. 881–885 (2008).
116. Menger K.: Zur allgemeinen kurventheorie. Fund Math. **10**, 96–115 (1927).
117. Metsch K.: Bose–Burton type theorems for finite projective, affine and polar spaces. In: Lamb J.D., Preece D.A. (eds.) Surveys in Combinatorics 1999. London Mathematical Society Lecture Note Series, vol. 267, pp. 137–166. Cambridge University Press, Cambridge (1999).
118. Metsch K.: Blocking sets in projective spaces and polar spaces. J. Geom. **76**, 216–232 (2003).
119. Metsch K.: Blocking subspaces by lines in PG(n, q). Combinatorica **24**, 459–486 (2004).
120. Miyakawa M., Munemasa A., Yoshiara S.: On a class of small 2-designs over GF(q). J. Comb. Des. **3**, 61–77 (1995).
121. Motwani R., Raghavan P.: Randomized Algorithms. Cambridge University Press, Cambridge (1995).
122. Nakić A., Pavčević M.O.: Tactical decompositions of designs over finite fields. Des. Codes Cryptogr. **77**, 49–60 (2015).
123. Oggier F.: Some Constructions of Storage Codes from Grassmann Graphs. ETH-Zurich, Zurich (2014). doi:10.3929/ethz-a-010094830.
124. Oggier F., Datta A.: Self-repairing codes for distributed storage - A projective geometric construction. In: Information Theory Workshop (ITW), pp. 30–34 (2011).
125. Olmez O., Ramamoorthy A.: Fractional repetition codes with flexible repair from combinatorial designs. arXiv:1408.5780v1 (August 2014).
126. Penttila T., Williams B.: Regular Packings of PG(3, q). Eur. J. Comb. **19**, 713–720 (1998).
127. Pepe V., Storme L.: The use of blocking sets in Galois geometries and in related research areas. In: Narasimha, Sastry N.S. (ed.). Springer Proceedings in Mathematics. Proceedings of the Satellite Conference Buildings, Finite Geometries and Groups of the International Congress of Mathematicians 2010, Bangalore, India (29–31, August, 2010), vol. 10, pp. 305–327 (2012).
128. QR- CODES: http://raidenii.net/files/datasheets/misc/qr_code.pdf.
129. Rashmi K.V., Shah N.B., Kumar P.V., Ramchandran K.: Explicit construction of optimal exact regenerating codes for distributed storage. In: 47th Annual Allerton Conference on Communications, Control and Computing, pp. 1243–1249 (2009).
130. Raviv N., Etzion T.: Distributed storage systems based on intersecting subspace codes. In: International Symposium on Information Theory, pp. 1462–1466 (2015). arXiv:1406.6170 (June 2014).
131. Riis S., Ahlswede R.: Problems in Network Coding and Error Correcting Codes. Appended by a draft version of Riis S.: Utilising public information in network coding. General Theory of Information Transfer and Combinatorics. In: Lecture Notes in Computer Science, vol. 4123, pp. 861–897 (lecture 3) (2006).
132. Rodier F., Sboui A.: Les arrangements minimaux et maximaux d'hyperplans dans $\mathbb{P}^n(\mathbb{F}_q)$. C. R. Acad. Sci. Paris Ser. I **344**, 287–290 (2007).
133. Rosenthal J., Silberstein N., Trautmann A.-L.: On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes. Des. Codes Cryptogr. **73**, 393–416 (2014).

134. Roth R.M.: Maximum-rank array codes and their application to crisscross error correction. IEEE Trans. Inf. Theory **37**, 328–336 (1991).
135. Sarmiento J.: Resolutions of PG(5,2) with point-cyclic automorphism group. J. Comb. Des. **8**, 2–14 (2000).
136. Sarmiento J.: On point-cyclic resolutions of the $2-(63,7,15)$ design associated with PG(5,2). Gr. Comb. **18**, 621–632 (2002).
137. Sboui A.: Special numbers of rational points on hypersurfaces in the n-dimensional projective space over a finite field. Discret. Math. **309**, 5048–5059 (2009).
138. Schönheim J.: On coverings. Pac. J. Math. **14**, 1405–1411 (1964).
139. Schwartz M., Etzion T.: Codes and anticodes in the Grassman graph. J. Comb. Theory, Ser. A **97**, 27–42 (2002).
140. Segre B.: Ovals in a finite projective plane. Can. J. Math. **7**, 414–416 (1955).
141. Serre J.-P.: Lettre à M. Tsfasman du 24 Juillet 1989. Journées Arithmétiques de Luminy 17-21 Juillet 1989. Astérisque **198-199-200**, 11 (1991), 351–353 (1992).
142. Silberstein N., Etzion T.: Fractional repetition codes for repair in distributed storage systems. arXiv:1401.4734v3 (January 2014)
143. Silva D., Kschischang F.R.: On metrics for error-correction in network coding. IEEE Trans. Inf. Theory **55**, 5479–5490 (2009).
144. Silva D., Kschischang F.R., Koetter R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory **54**, 3951–3967 (2008).
145. Skachek V.: Recursive code construction for random networks. IEEE Trans. Inf. Theory **56**, 1378–1382 (2010).
146. Solomon G., Stiffler J.J.: Algebraically punctured cyclic codes. Inf. Control **8**, 170–179 (1965).
147. Sørensen A.B.: Projective Reed–Muller codes. IEEE Trans. Inf. Theory **37**, 1567–1576 (1991).
148. Suzuki H.: 2-Designs over GF(2^m). Gr. Comb. **6**, 293–296 (1990).
149. Suzuki H.: On the inequalities of t-designs over a finite field. Eur. J. Comb. **11**, 601–607 (1990).
150. Suzuki H.: 2-Designs over GF(q). Gr. Comb. **8**, 381–389 (1992).
151. Sziklai P.: On small blocking sets and their linearity. J. Comb. Theory Ser. A **115**, 1167–1182 (2008).
152. Szőnyi T.: Blocking sets in Desarguesian affine and projective planes. Finite Fields Appl. **3**, 187–202 (1997).
153. Szőnyi T., Weiner Zs.: Small blocking sets in higher dimensions. J. Comb. Theory Ser. A **95**, 88–101 (2001).
154. Thomas S.: Designs over finite fields. Geom. Dedicata **21**, 237–242 (1987).
155. Thomas S.: Designs and partial geometries over finite fields. Geom. Dedicata **63**, 247–253 (1996).
156. Tits J.: Sur les analogues algébriques des groupes semi-simples complexes. Colloque d'Algèbre Supérieure, tenu á Bruxelles du 19 au 22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain. Librairie Gauthier-Villars, Paris, pp. 261–289 (1957).
157. Topalova S., Zhelezova S.: 2-spreads and transitive and orthogonal 2-parallelisms of PG(5,2). Gr. Comb. **26**, 727–735 (2010).
158. Trautmann A.-L.: Isometry and automorphisms of constant dimension codes. Adv. Math. Commun. **7**, 147–160 (2013).
159. Trautmann A.-L., Rosenthal J.: A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. Des. Codes Cryptogr. **66**, 275–289 (2013).
160. Trautmann A.-L., Manganiello F., Braun M., Rosenthal J.: Cyclic orbit codes. IEEE Trans. Inf. Theory **59**, 7386–7404 (2013).
161. Wang J.: Quotient sets and subset-subspace analogy. Adv. Appl. Math. **23**, 333–339 (1999).
162. Wang H., Xing C., Safavi-Naini R.M.: Linear authentication codes: bounds and constructions. IEEE Trans. Inf. Theory **49**, 866–872 (2003).
163. Wachter-Zeh A., Etzion T.: Optimal Ferrers Diagram Rank-Metric Codes. arXiv:1405.1885 (May 2014).
164. Xia S.-T., Fu F.-W.: Johnson type bounds on constant dimension codes. Des. Codes Cryptogr. **50**, 163–172 (2009).
165. Zaicev G.V., Zinoviev V.A., Semakov N.V.: Interrelations of Preparata and Hamming codes and extension of Hamming codes to new double error-correcting codes. In: Proceedings of the 2nd International Symposium on Information Theory, Budapest, pp. 257–263 (1971).
166. Zhang Z.: Theory and applications of network error correction coding. Proc. IEEE **99**, 406–420 (2011).