Subspace Codes

Azadeh Khaleghi, Danilo Silva, and Frank R. Kschischang

Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario M5S 3G4, Canada
{azalea, danilo, frank}@comm.utoronto.ca

Abstract. This paper is a survey of bounds and constructions for subspace codes designed for the injection metric, a distance measure that arises in the context of correcting adversarial packet insertions in linear network coding. The construction of lifted rank-metric codes is reviewed, along with improved constructions leading to codes with strictly more codewords. Algorithms for encoding and decoding are also briefly described.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of size q, and let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$. The set of all subspaces of $\mathbb{F}_q^n$, called the *projective space* of order n over $\mathbb{F}_q$, is denoted $\mathcal{P}_q(n)$. The set of all k-dimensional subspaces of $\mathbb{F}_q^n$, called a *Grassmannian*, is denoted $\mathcal{G}_q(n,k)$, where $0 \leq k \leq n$. Obviously $\mathcal{P}_q(n) = \bigcup_{k=0}^{n} \mathcal{G}_q(n,k)$.

A *(subspace) code* $\mathcal{C}$ is a nonempty collection of subspaces of $\mathbb{F}_q^n$, i.e., a non-empty subset of $\mathcal{P}_q(n)$. Unlike classical coding theory, where each codeword is a vector, here each codeword of $\mathcal{C}$ is itself an entire space of vectors. A code in which each codeword has the same dimension, i.e., a code contained within a single Grassmannian, is called a *constant-dimension* code.

As in classical coding theory, it is important to define a distance measure between codewords. One possible distance measure between two spaces U and V in $\mathcal{P}_q(n)$—though not the metric of main interest in this paper—is the so-called *subspace metric*

$$\mathsf{d}_{\mathrm{S}}(U,V) \triangleq \mathsf{dim}(U) + \mathsf{dim}(V) - 2\,\mathsf{dim}(U \cap V),$$

introduced in the context of error- and erasure-correction in linear network coding [1]. The measure that will be of main interest here, however, is the *injection distance* $\mathsf{d}(U,V)$, introduced in the later paper [2], and given by

$$\mathsf{d}(U,V) \triangleq \mathsf{max}\{\mathsf{dim}(U), \mathsf{dim}(V)\} - \mathsf{dim}(U \cap V).$$

This function is indeed a metric on $\mathcal{P}_q(n)$ [2]. The injection distance and the subspace distance are closely related, as

$$\mathsf{d}(U,V) = \frac{1}{2}\mathsf{d}_{\mathrm{S}}(U,V) + \frac{1}{2}|\,\mathsf{dim}(V) - \mathsf{dim}(U)|, \quad \forall U,V \in \mathcal{P}_q(n). \tag{1}$$

In fact, the two metrics are equivalent when U and V have the same dimension, i.e., if $\mathsf{dim}(U) = \mathsf{dim}(V)$ then $\mathsf{d}_{\mathrm{S}}(U,V) = 2\,\mathsf{d}(U,V)$. Denote by $U+V$ the sum of U and V, i.e., let $U+V = \{u+v\colon u \in U,\ v \in V\}$. The relation $\mathsf{dim}(U+V) = \mathsf{dim}(U) + \mathsf{dim}(V) - \mathsf{dim}(U \cap V)$ gives the alternative expressions

$$\begin{aligned}\mathsf{d}(U,V) &= \mathsf{dim}(U+V) - \mathsf{min}\{\mathsf{dim}(U),\mathsf{dim}(V)\} \text{ and}\\ \mathsf{d}_{\mathrm{S}}(U,V) &= 2\,\mathsf{dim}(U+V) - \mathsf{dim}(U) - \mathsf{dim}(V)\\ &= \mathsf{dim}(U+V) - \mathsf{dim}(U \cap V)\end{aligned}$$

for two metrics.

The minimum distance between distinct codewords in a code $\mathcal{C}$ is denoted as $\mathsf{d}(\mathcal{C})$ if the injection metric is used and as $\mathsf{d}_{\mathrm{S}}(\mathcal{C})$ if the subspace metric is used, i.e.,

$$\mathsf{d}(\mathcal{C}) \triangleq \mathsf{min}_{U,V\in\mathcal{C}\colon U\neq V}\ \mathsf{d}(U,V) \text{ and } \mathsf{d}_{\mathrm{S}}(\mathcal{C}) \triangleq \mathsf{min}_{U,V\in\mathcal{C}\colon U\neq V}\ \mathsf{d}_{\mathrm{S}}(U,V).$$

It follows from (1) that

$$\mathsf{d}(\mathcal{C}) \geq \frac{1}{2}\mathsf{d}_{\mathrm{S}}(\mathcal{C}), \tag{2}$$

with equality if (but not only if) $\mathcal{C}$ is a constant dimension code.

A code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is called an $(n,d)_q$ code if $\mathsf{d}(\mathcal{C}) = d$, and is called an $(n,d,k)_q$ code if, additionally, $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$. Similarly, $\mathcal{C}$ is called an $(n,d)_q^{\mathrm{S}}$ code if $\mathsf{d}_{\mathrm{S}}(\mathcal{C}) = d$. The latter notation follows the convention, used throughout this paper, that if a concept is defined for the injection metric, then the analogous concept for the subspace metric is denoted by a superscript S. We will, however, have no occasion to refer to an $(n,d,k)_q^{\mathrm{S}}$ code, since such a code is an $(n,d/2,k)_q$ code. We denote by $A_q(n,d)$ and $A_q(n,d,k)$ the sizes of a largest $(n,d)_q$ code and a largest $(n,d,k)_q$ code, respectively.

Subspace codes turn out to be the natural objects in several applications, such as noncoherent linear network coding [1–5] and linear authentication [6, 7]. For linear authentication, it is shown in [6, Theorem 4.1] that every $(n,d,k)_q$ code $\mathcal{C}$ is an $[n,|\mathcal{C}|,n-k,d]$ linear authentication code over $\mathbb{F}_q$, and vice-versa. For network coding, it is shown in [2, Theorem 20] that an $(n,d)_q$ code can correct any t corrupt packets injected in a noncoherent linear network coding system with rank deficiency ρ if and only if $d > 2t + \rho$. Thus, the packet-error correction capability of a subspace code for network coding is completely characterized in terms of the injection distance. Historically, the subspace distance appeared earlier in this context [1], but it can only provide a correction guarantee (not the converse), which can be seen from (2).

This paper surveys the existing literature on constructions of $(n, d)_q$ and $(n, d, k)_q$ codes, as well as upper and lower bounds on $A_q(n, d)$ and $A_q(n, d, k)$. Usually, results for general subspace codes are based on previous results for constant-dimension codes. In view of (2), results for the subspace metric may also be useful and are reviewed as well.

The remainder of the paper is organized as follows. Section 2 establishes some useful notation and reviews properties of rank metric codes. Section 3 discusses bounds on $A_q(n, d)$, $A_q(n, d, k)$ and $A_q^{\mathrm{S}}(n, d)$. Section 4 reviews existing constructions of general and constant-dimension subspace codes. Section 5 briefly describes encoding and decoding methods for subspace codes. The paper ends in Section 6 with some concluding remarks and a list of open problems.

2 Preliminaries

2.1 Notation and Basic Facts

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$. If $\mathcal{A}$ is a finite set, let $|\mathcal{A}|$ denote its cardinality.

We will often need to refer to vectors and matrices with components from $\mathbb{F}_q$. If $v = (v_1, \ldots, v_n)$ is a vector $\mathbb{F}_q^n$, let $\mathsf{supp}(v) = \{i \in \{1, \ldots, n\} \colon v_i \neq 0\}$ denote its support and let $\mathsf{wt}(v) = |\,\mathsf{supp}(v)|$ denote its Hamming weight.

Let $\mathbb{F}_q^{m \times n}$ denote the set of all $m \times n$ matrices over $\mathbb{F}_q$. For concreteness, a vector in $\mathbb{F}_q^n$ will be considered as an element of $\mathbb{F}_q^{1 \times n}$, i.e., as a row vector. The $m \times n$ all-zero matrix and the $n \times n$ identity matrix are denoted by $\mathbf{0}_{m \times n}$ and $I_{n \times n}$, respectively, where the subscripts may be omitted when there is no risk of confusion.

Let $X \in \mathbb{F}_q^{m \times n}$ be an $m \times n$ matrix. If $\mathcal{S}$ is a nonempty subset of $\{1, \ldots, m\}$, then $X_{\mathcal{S}}$ is the submatrix of X consisting of the rows indexed by $\mathcal{S}$ (in increasing order). If X is nonzero, then its reduced row echelon form (RREF) is denoted as $\mathsf{rref}(X)$. Associated with a nonzero X is a vector $\mathsf{prof}(X) \in \{0, 1\}^n$, called the *profile vector* of X, in which $\mathsf{supp}(\mathsf{prof}(X))$ is the set of column positions of the leading ones in the rows of $\mathsf{rref}(X)$. If $X = \mathbf{0}$, then we set $\mathsf{prof}(X)$ to the zero vector.

The row space of a matrix X is denoted as $\langle X\rangle$. If $X \in \mathbb{F}_q^{m\times n}$ then $\langle X\rangle \in \mathcal{P}_q(n)$. The rank of X is denoted as $\mathsf{rank}(X)$ and, of course, $\mathsf{rank}(X) = \mathsf{dim}\left(\langle X\rangle\right)$. More generally, if $X \in \mathbb{F}_q^{n\times m}$ and $Y \in \mathbb{F}_q^{N\times m}$, then

$$\left\langle \begin{bmatrix} X \\ Y \end{bmatrix} \right\rangle = \langle X\rangle + \langle Y\rangle\,;$$

therefore,

$$\mathsf{rank}\begin{bmatrix} X \\ Y \end{bmatrix} = \mathsf{dim}(\langle X\rangle + \langle Y\rangle).$$

Note that $\mathsf{wt}(\mathsf{prof}(X)) = \mathsf{rank}(X)$.

Associated with a vector space $U \in \mathcal{G}_q(n,k)$, $k > 0$, is a unique $k \times n$ matrix X_U in RREF (i.e., with $X_U = \mathsf{rref}(X_U)$) having the property that $\langle X_U\rangle = U$. With a slight abuse of notation we extend the prof function to vector spaces by defining

$$\mathsf{prof}(U) \triangleq \mathsf{prof}(X_U),$$

where $\mathsf{prof}(U)$ is the zero vector if $\mathsf{dim}(U) = 0$. Given any binary profile vector $b \in \{0,1\}^n$, the so-called *Schubert cell* [8] in $\mathcal{P}_q(n)$ corresponding to b is the set

$$\mathcal{S}_q(b) = \mathsf{prof}^{-1}(b) = \{U \in \mathcal{P}_q(n) : \mathsf{prof}(U) = b\}.$$

If $\mathsf{wt}(b) = k$, then $\mathcal{S}_q(b) \subseteq \mathcal{G}_q(n,k)$. Thus binary profile vectors (in general) induce a *partition* of $\mathcal{P}_q(n)$ into 2^n distinct Schubert cells, while binary profile vectors of weight k (in particular) induce a partition of $\mathcal{G}_q(n,k)$ into $\binom{n}{k}$ Schubert cells. These partitions will become useful in Section 4.

Associated with $\mathcal{G}_q(n,k)$ is a distance-regular graph (called a Grassmann graph) whose vertices correspond to the elements of $\mathcal{G}_q(n,k)$ and where two vertices are adjacent if the corresponding subspaces intersect in a space of dimension $k-1$ [9]. The Grassmannian $\mathcal{G}_q(n,k)$ also forms an association scheme, the so-called q-Johnson scheme [10, Ch. 30], in which two spaces are ith associates if they intersect in a space of dimension $k-i$, or, equivalently, if they are separated by graph distance i in the Grassmann graph. When restricted to $\mathcal{G}_q(n,k)$, the injection distance $\mathsf{d}(\cdot,\cdot)$ corresponds to the graph distance in the corresponding Grassmann graph.

It is well known that the cardinality of the Grassmannian $\mathcal{G}_q(n,k)$ is given by the *Gaussian coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{(q^n - q^i)}{(q^k - q^i)}.$$

The subscript q will be omitted when there is no possibility of confusion. Note that $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$ and $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$.

Let $V \in \mathcal{G}_q(n,k)$ be a fixed vector space of dimension k, and let $N_q(n,k,j,\ell)$ denote the number of elements $W \in \mathcal{G}_q(n,j)$ with the property that $V \cap W \in \mathcal{G}_q(n,\ell)$. We have

$$N_q(n,k,j,\ell) = q^{(k-\ell)(j-\ell)} \begin{bmatrix} k \\ \ell \end{bmatrix} \begin{bmatrix} n-k \\ j-\ell \end{bmatrix}. \tag{3}$$

To see this, observe that the space U of intersection can be chosen in $\begin{bmatrix} k \\ \ell \end{bmatrix}$ ways. This subspace can be extended to a j-dimensional subspace in

$$\frac{(q^n - q^k)(q^n - q^{k+1})(q^n - q^{k+2}) \cdots (q^n - q^{k+j-\ell-1})}{(q^j - q^\ell)(q^j - q^{\ell+1})(q^j - q^{\ell+2}) \cdots (q^j - q^{j-1})} = q^{(j-\ell)(k-\ell)} \begin{bmatrix} n-k \\ j-l \end{bmatrix}$$

ways, since we can extend U by adjoining any of the $q^n - q^k$ vectors not in V, then adjoining any of the $q^n - q^{k+1}$ vectors not in the resulting $(k+1)$-space, etc., but any specific choice is in an equivalent class of size $(q^j - q^\ell)(q^j - q^{\ell+1}) \cdots (q^j - q^{j-1})$.

The quantity $N_q(n,k,j,\ell)$ is very useful. For example, $N_q(n,n,k,k) = \begin{bmatrix} n \\ k \end{bmatrix}$ (the number of k-subspaces of an n-space, i.e., $|\mathcal{G}_q(n,k)|$), $N_q(n,k,j,k) = \begin{bmatrix} n-k \\ j-k \end{bmatrix}$ (the number of j-dimensional spaces containing the k-space V), $N_q(n,k,k,k-i) = q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}$ (the number of k-spaces at injection distance i from the k-space V), etc.

Let us also mention here two additional properties of the Gaussian coefficient [11]

$$\begin{bmatrix} m \\ n \end{bmatrix} \begin{bmatrix} n \\ t \end{bmatrix} = \begin{bmatrix} m \\ t \end{bmatrix} \begin{bmatrix} m-t \\ n-t \end{bmatrix}, \quad t \le n \le m, \tag{4}$$

and [1, Lemma 5]

$$q^{i(n-i)} \le \begin{bmatrix} n \\ i \end{bmatrix} \le h(q) q^{i(n-i)}, \tag{5}$$

where $h(q) = \prod_{j=0}^{\infty} \frac{1}{1-q^{-j}}$. It is shown in [1] that $h(q)$ decreases monotonically with q, approaching $q/(q-1)$ for large q. The series for $h(q)$ converges rapidly; the following table lists $h(q)$ for various values of q.

q	2	3	4	5	7	8	9	11	16	32	64	128	256
$h(q)$	3.46	1.79	1.45	1.32	1.20	1.16	1.14	1.11	1.07	1.03	1.02	1.01	1.004

2.2 Rank-Metric Codes

For matrices $X, Y \in \mathbb{F}_q^{n\times m}$, the *rank distance* is defined as

$$\mathsf{d}_{\mathrm{R}}(X,Y) \triangleq \mathsf{rank}(Y-X).$$

As observed in [11], the rank distance is indeed a metric. A *rank-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ is a matrix code (i.e., a nonempty set of matrices) used in the context of the rank metric. We use $\mathsf{d}_{\mathrm{R}}(\mathcal{C})$ to denote the minimum rank distance of $\mathcal{C}$. The Singleton bound for the rank metric [11, 12] (see also [3, 13, 14]) states that

$$|\mathcal{C}| \leq q^{\mathsf{max}\{n,m\}(\mathsf{min}\{n,m\}-d+1)}$$

for every code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ with $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$. Codes that achieve this bound are called *maximum-rank-distance* (MRD) codes and linear MRD codes are known to exist for all choices of parameters q, n, m and $d \leq \mathsf{min}\{n,m\}$ [11].

Gabidulin codes [11] are an important class of MRD codes, described as follows. Without loss of generality, assume $n \leq m$ (otherwise consider the transposed version of the following argument). Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$, and let $\theta \colon \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ be a vector space isomorphism, where the elements in $\mathbb{F}_q^m$ are regarded as row vectors. Let $\mathbb{F}_{q,m}^n[x]$ denote the set of linearized polynomials, i.e., all polynomials of the form $f(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$, where $f_i \in \mathbb{F}_{q^m}$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ be elements that are linearly independent when regarded as vectors in $\mathbb{F}_q^m$, and let $0 \leq d \leq n$.

A *Gabidulin code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ is defined as

$$\mathcal{C} = \left\{ c \in \mathbb{F}_q^{n\times m} \colon c = \left[\theta(f(\alpha_1)), \ldots, \theta(f(\alpha_n))\right]^T,\ f(x) \in \mathbb{F}_{q,m}^{(n-d+1)}[x] \right\}.$$

It is shown in [11] that such a code has $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$, so it is indeed an MRD code.

Given a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$, a minimum-rank-distance decoder for $\mathcal{C}$ takes a matrix $r \in \mathbb{F}_q^{n\times m}$ and returns a codeword $c \in \mathcal{C}$ that minimizes the rank distance $\mathsf{d}_{\mathrm{R}}(c,r)$. It is easy to see that, if $\mathsf{d}_{\mathrm{R}}(c,r) < \mathsf{d}_{\mathrm{R}}(\mathcal{C})/2$ for some $c \in \mathcal{C}$, then c is the unique solution to the above problem. A bounded-distance decoder for $\mathcal{C}$ returns $c \in \mathcal{C}$ if $\mathsf{d}_{\mathrm{R}}(c,r) < \mathsf{d}_{\mathrm{R}}(\mathcal{C})/2$, or declares a failure if no such codeword can be found. For Gabidulin codes, very efficient bounded-distance decoders exist; see, e.g., [3, 11].

3 Bounds

In this section, we consider bounds on $A_q(n,d,k)$, $A_q(n,d)$, and $A_q^{\mathrm{S}}(n,d)$. Since

$$A_q(n,d,k) = A_q(n,d,n-k), \tag{6}$$

when dealing with $A_q(n,d,k)$, we may safely assume $k \le n/2$.

3.1 Upper Bounds on $A_q(n,d,k)$

Sphere-Packing Bound: The simplest upper bound that can be obtained for $A_q(n,d,k)$ is the sphere-packing bound, which follows from the fact that the Grassmann graph corresponding to $\mathcal{G}_q(n,k)$ is distance-regular. First, we need the concept of a sphere in $\mathcal{G}_q(n,k)$.

For $V \in \mathcal{G}_q(n,k)$, let $\mathcal{B}_V(t,k) \triangleq \{U \in \mathcal{G}_q(n,k)\colon \mathsf{d}(V,U) \le t\}$ be the set of all subspaces of dimension k at injection distance at most t from V, a set that we regard as a sphere in $\mathcal{G}_q(n,k)$ of radius t with center V. For any $V \in \mathcal{G}_q(n,k)$, the size of $\mathcal{B}_V(t,k)$ is [1]

$$|\mathcal{B}_V(t,k)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}, \tag{7}$$

which follows easily from (3). Note that the size of a sphere in $\mathcal{G}_q(n,k)$ is independent of its center. For convenience, define $B(t,k) \triangleq |\mathcal{B}_V(t,k)|$.

The following sphere-packing bound for $A_q(n,d,k)$ is given in [1].

Theorem 1 (Sphere-packing bound).

$$A_q(n,d,k) \le \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{B(\lfloor (d-1)/2 \rfloor, k)}.$$

Singleton Bound: In [1] a puncturing operation in $\mathcal{G}_q(n,k)$ is defined that reduces by one the dimension of the ambient space and the dimension of each subspace in $\mathcal{G}_q(n,k)$. According to this puncturing operation, a punctured code obtained by puncturing an $(n,d,k)_q$ code is itself an $(n-1,d',k-1)_q$ code, where $d' \ge d-1$. If an $(n,d,k)_q$ code is punctured $d-1$ times repeatedly, an $(n-d+1,d'',k-d+1)_q$ code (with $d'' \ge 1$) is obtained, which may have size no greater than $|\mathcal{G}_q(n-d+1,k-d+1)|$. Thus the following Singleton-type bound is established [1].

Theorem 2 (Singleton bound).

$$A_q(n,d,k) \le |\mathcal{G}_q(n-d+1,k-d+1)| = \begin{bmatrix} n-d+1 \\ k-d+1 \end{bmatrix} = \begin{bmatrix} n-d+1 \\ n-k \end{bmatrix}.$$

We note that from (5) it follows that

$$A_q(n,d,k) \leq h(q)q^{(n-k)(k-d+1)}. \tag{8}$$

It is observed in [1] that this bound is always stronger than the sphere-packing bound of Theorem 1 for nontrivial codes.

Anticode Bound: Since $\mathcal{G}_q(n,k)$ is an association scheme, the anticode bound of Delsarte [15] can be applied. Let $\mathcal{C}$ be an $(n,d,k)_q$ code. Then Delsarte's bound implies that

$$|\mathcal{C}| \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}|},$$

where $\mathcal{A} \subseteq \mathcal{G}_q(n,k)$ is any set with maximum distance $d-1$ (called an *anticode*).

Note that, for all $U,V \in \mathcal{G}_q(n,k)$, $\mathsf{d}(U,V) \leq d-1$ if and only if $\mathsf{dim}(U \cap V) \geq k-d+1$. Thus, we can take $\mathcal{A}$ as a set in which any two elements intersect in a space of dimension at least $k-d+1$. From the results of Frankl and Wilson [16], it follows that, for $k \leq n/2$, the maximum value of $|\mathcal{A}|$ is equal to $\begin{bmatrix} n-k+d-1 \\ d-1 \end{bmatrix}$. Hence, we have the following bound.

Theorem 3 (Anticode bound).

$$A_q(n,d,k) \leq \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\begin{bmatrix} n-k+d-1 \\ d-1 \end{bmatrix}} = \frac{\begin{bmatrix} n \\ k-d+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-d+1 \end{bmatrix}}.$$

The equality in this theorem follows by observing from (4) that $\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} k \\ k-d+1 \end{bmatrix} = \begin{bmatrix} n \\ k-d+1 \end{bmatrix}\begin{bmatrix} n-k+d-1 \\ d-1 \end{bmatrix}$. Applying (5) yields (8).

It is easy to observe that Delsarte's bound also implies the sphere-packing bound as a special case, since a sphere $\mathcal{B}_V(\lfloor (d-1)/2 \rfloor, k)$ is (by the triangle inequality) an anticode of maximum distance $d-1$. However, a sphere is not an optimal anticode in $\mathcal{G}_q(n,k)$, and therefore the bound of Theorem 3 is always tighter for nontrivial codes.

The bound in Theorem 3 was first obtained by Wang, Xing and Safavi-Naini in [6] using a different argument. The proof that Theorem 3 follows from Delsarte's bound is due to Etzion and Vardy [17].

As observed in [7], the anticode bound is always stronger than the Singleton bound for non-trivial codes in $\mathcal{G}_q(n,k)$.

Johnson-Type Bounds: Associated with an $(n, d, k)_q$ code $\mathcal{C}$ is a binary constant weight code of length $q^n - 1$, weight $q^k - 1$, and minimum Hamming distance $2q^k(1 - q^{-d})$, having $|\mathcal{C}|$ codewords. This binary code has codewords that form the rows of the $|\mathcal{C}| \times (q^n - 1)$ incidence matrix between codewords of $\mathcal{C}$ and the nonzero vectors of $\mathbb{F}_q^n$. The classical Johnson bound on binary constant weight codes (e.g., see [18]) immediately implies the following bound on $A_q(n, d, k)$.

Theorem 4 **([7]).**

$$A_q(n, d, k) \leq \frac{q^k(1 - q^{-d})(q^n - 1)}{(q^k - 1)^2 - (q^n - 1)(q^k - 1) + q^k(1 - q^{-d})(q^n - 1)}.$$

Now let $\mathcal{C}$ be an $(n, d, k)_q$ code with $A_q(n, d, k)$ codewords. For any subspace $U \in \mathcal{G}_q(n, n-1)$ of dimension $n-1$, let $\mathcal{C}_U$ be the set of codewords of $\mathcal{C}$ contained entirely in U. Clearly $\mathcal{C}_U$ is an $(n - 1, d, k)_q$ code, and so cannot have cardinality greater than $A_q(n - 1, d, k)$. If we now form the summation of such cardinalities, ranging over all possible U, we obtain

$$\sum_{U \in \mathcal{G}_q(n, n-1)} |\mathcal{C}_U| = \left(\frac{q^{n-k} - 1}{q - 1}\right) A_q(n, d, k) \leq \left(\frac{q^{n-1} - 1}{q - 1}\right) A_q(n - 1, d, k),$$

where the first equality follows from the fact that each codeword of $\mathcal{C}$ will appear as a codeword in exactly $(q^{n-k} - 1)/(q - 1)$ of the $\mathcal{C}_U$'s. This argument yields the following theorem [17].

Theorem 5 **([17]).**

$$A_q(n, d, k) \leq \frac{q^n - 1}{q^{n-k} - 1} A_q(n - 1, d, k)$$

Applying (6) results in the following.

Theorem 6 **([7, 17]).**

$$A_q(n, d, k) \leq \frac{q^n - 1}{q^k - 1} A_q(n - 1, d, k - 1)$$

Theorems 5 and 6 may be iterated to give an upper bound for $A_q(n, d, k)$. However, as in the classical case of the Johnson space, the order in which the two bounds should be iterated in order to get the tightest bound is unclear. By iterating Theorem 6 with itself, the following bound is established in [7, 17].

Theorem 7 ([7, 17]).

$$A_q(n,d,k) \le \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+d}-1}{q^d-1} \right\rfloor \cdots \right\rfloor \right\rfloor .$$

It is shown in [7] that Theorem 5 improves on the anticode bound.

Ahlswede and Aydinian Bound: Let D be a nonempty subset of $\{1,\ldots,n\}$ and let $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ be a code. If, for all $U, V \in \mathcal{C}$, with $U \ne V$, we have $\mathsf{d}(U,V) \in D$, then we say that $\mathcal{C}$ is a code with distances in D. The following Lemma is given in [19].

Lemma 1 ([19]). *Let $\mathcal{C}_D \subseteq \mathcal{G}_q(n,k)$ be a code with distances from a set D. Then, for a nonempty subset $\mathcal{B} \subseteq \mathcal{G}_q(n,k)$ there exists a code $\mathcal{C}_D^*(\mathcal{B}) \subseteq \mathcal{B}$ with distances from D such that*

$$\frac{|\mathcal{C}_D^*(\mathcal{B})|}{|\mathcal{B}|} \ge \frac{|\mathcal{C}_D|}{\left[{n \atop k}\right]},$$

where, if $|\mathcal{C}_D^*| = 1$, then $\mathcal{C}_D^*$ is a code with distances from D by convention.

In particular when $\mathcal{C}_D$ is an $(n,d,k)_q$ code and $\mathcal{B}$ is an anticode of maximum distance $d-1$, then $|\mathcal{C}_D^*(\mathcal{B})| = 1$ and Delsarte's anticode bound on $\mathcal{G}_q(n,k)$ is obtained.

Using Lemma 1 Ahlswede and Aydinian obtain the following bound:

Theorem 8 ([19]). *For integers $0 \le t \le d \le k$, $k-t \le m \le n$,*

$$A_q(n,d,k) \le \frac{\left[{n \atop k}\right] A_q(m,d-t,k-t)}{\sum\limits_{i=0}^{t} q^{i(m-i)} \begin{bmatrix} m \\ k-i \end{bmatrix} \begin{bmatrix} n-m \\ i \end{bmatrix}}$$

It is shown in [19] that for $t = 0$ and $m = n-1$, Theorem 8 gives Theorem 5.

3.2 Upper Bounds on $A_q(n,d)$ and $A_q^{\mathrm{S}}(n,d)$

A Simple Bound: The simplest upper bound in $A_q(n,d)$ follows immediately from the observation that every subspace code is a union of constant-dimension codes, and hence

$$A_q(n,d) \le \sum_{k=0}^{n} A_q(n,d,k)$$

Etzion-Vardy LP Bound: Etzion and Vardy derive in [17] the following linear programming bound for $A_q^{\mathrm{S}}(n,3)$.

Theorem 9 **([17]).** *Let* $f^* = \mathsf{max}(\sum_{i=0}^{n} D_i)$ *subject to the following linear constraints:*

$$\frac{q^{n-i+1}-1}{q-1} D_{i-1} + D_i + \frac{q^{i+1}-1}{q-1} D_{i+1} \leq \begin{bmatrix} n \\ i \end{bmatrix} \tag{9}$$

and $D_i \leq A_q(n,2,i)$, *for all* $i = 0, 1, \cdots, n$, *where* $D_{-1} = D_{n+1} = 0$ *by convention. Then*

$$A_q^{\mathrm{S}}(n,3) \leq f^*.$$

Ahlswede-Aydinian LP Bound: Ahlswede and Aydinian establish the following linear programming bound for $A_q(n,d)$ in [19].

Theorem 10 **([19]).** *For integers* $1 \leq d \leq \frac{n}{2}$, *let*

$$f(n,d,q) = \mathsf{max}(\sum_{i=0}^{n} f_i)$$

subject to the following linear constraints:

$f_i \in \mathbb{N}$ *for* $i = 0, 1, \ldots, n.$

$f_0 = f_n = 1,\ f_k = f_{n-k} = 0$ *for* $k = 1, \ldots, d$

$f_{-j} = f_{n+j} = 0$ *for* $j = 1, \ldots, d$ *(by convention)*

$f_k + \frac{1}{d+1} \sum_{i=1}^{d} (d+1-i) \left(f_{k-i} \begin{bmatrix} n-k+i \\ n-k \end{bmatrix} + f_{k+i} \begin{bmatrix} k+i \\ k \end{bmatrix} \right) \leq \begin{bmatrix} n \\ k \end{bmatrix}$ *and,*

$f_k \leq A_q(n, d+1, k)$ *for* $k = 0, \ldots, n.$

Then,

$$A_q(n,d) \leq f(n,d,q).$$

3.3 Lower Bounds

In this section, we give the counterparts of the Gilbert-Varshamov lower bound for $A_q(n,d,k)$, $A_q(n,d)$ and $A_q^{\mathrm{S}}(n,d)$. We start with the sizes of spheres in $\mathcal{P}_q(n)$. Recall that the size of a sphere in $\mathcal{G}_q(n,k)$ was given in (7).

For $V \in \mathcal{P}_q(n)$, let $\mathcal{B}_V(t) \triangleq \{U \in \mathcal{P}_q(n) \colon \mathsf{d}(V,U) \leq t\}$ be the sphere of radius t centered at V in $\mathcal{P}_q(n)$. For any $V \in \mathcal{P}_q(n)$, the size of $\mathcal{B}_V(t)$ can be computed using (3) as [20]

$$|\mathcal{B}_V(t)| = \sum_{r=0}^{t} q^{r^2} \begin{bmatrix} k \\ r \end{bmatrix} \begin{bmatrix} n-k \\ r \end{bmatrix} + \sum_{j=1}^{r} q^{r(r-j)} \left(\begin{bmatrix} k \\ r \end{bmatrix} \begin{bmatrix} n-k \\ r-j \end{bmatrix} + \begin{bmatrix} n-k \\ r \end{bmatrix} \begin{bmatrix} k \\ r-j \end{bmatrix} \right) \tag{10}$$

where $k = \mathsf{dim}(V)$. Note that the size of a sphere in $\mathcal{P}_q(n)$ does not depend on the specific subspace at its center, but does depend on its dimension. For convenience, we use the notation $B_k(t) \triangleq |\mathcal{B}_V(t)|$, where $k = \mathsf{dim}(V)$.

We can also define the analogous concept of a sphere under the subspace distance, which is denoted as $\mathcal{B}_V^{\mathrm{S}}(t)$ for $V \in \mathcal{P}_q(n)$. It is shown in [17] that

$$|\mathcal{B}_V^{\mathrm{S}}(t)| = \sum_{r=0}^{t} \sum_{j=0}^{r} q^{j(r-j)} \begin{bmatrix} n-k \\ r-j \end{bmatrix} \begin{bmatrix} k \\ j \end{bmatrix} \begin{bmatrix} n \\ k \end{bmatrix} \tag{11}$$

where $k = \mathsf{dim}(V)$. Similarly as above, we use the notation $B_k^{\mathrm{S}}(t) \triangleq |\mathcal{B}_V^{\mathrm{S}}(t)|$.

Let Ω be a general metric space with distance metric denoted by δ. Let $\mathcal{B}_\alpha(t) \triangleq \{\beta \in \Omega : \delta(\alpha,\beta) \leq t\}$ be a sphere of radius t centered at α in Ω. Every maximal code $\mathcal{C}$ of minimum distance d must satisfy

$$\sum_{c \in \mathcal{C}} |\mathcal{B}_c(d-1)| \geq |\Omega|. \tag{12}$$

Since the size $B(t,k)$ of a sphere $\mathcal{B}_V(t,k)$ in $\mathcal{G}_q(n,k)$ is independent of V, when Ω is replaced with $\mathcal{G}_q(n,k)$ and $\delta(\cdot,\cdot)$ with the injection metric, (12) results in the following Gilbert-Varshamov bound on $A_q(n,d,k)$.

Theorem 11 ([1]).

$$A_q(n,d,k) \geq \frac{|\mathcal{G}_q(n,k)|}{B(d-1,k)}. \tag{13}$$

Since by (11), the size of a sphere $\mathcal{B}_V(t)$ in $\mathcal{P}_q(n)$ depends on $\mathsf{dim}(V)$, the approach of Theorem 11 is not suitable for the derivation of a Gilbert-Varshamov bound in $\mathcal{P}_q(n)$.

As pointed out in [17], the appropriate framework for a Gilbert-Varshamov bound in spaces where the size of a sphere depends upon the location of its center is given by Tolhuizen [21]. Let $\overline{B}(t) \triangleq \frac{1}{|\Omega|} \sum_{\alpha \in \Omega} |\mathcal{B}_\alpha(t)|$ denote the "average size" of a sphere of radius t in Ω. Tolhuizen showed in [21] that the maximum size of a code $C \subseteq \Omega$ of minimum distance d is at least $\dfrac{|\Omega|}{\overline{B}(d-1)}$. Using this result along with (10), Khaleghi and Kschischang [20] and independently Gadouleau and Yan [14] obtain the following Gilbert-Varshamov bound for $A_q(n,d)$:

Theorem 12 ([14, 20]). $A_q(n,d) \geq \dfrac{|\mathcal{P}_q(n)|^2}{\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} B_k(d-1)}$.

Earlier, Etzion and Vardy [17] had already established the following Gilbert-Varshamov bound on $A_q^{\mathrm{S}}(n,d)$:

Theorem 13 ([17]). $A_q^{\mathrm{S}}(n,d) \geq \dfrac{|\mathcal{P}_q(n)|^2}{\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} B_k^{\mathrm{S}}(d-1)}$

where $B_k^{\mathrm{S}}(d-1)$ is given by (11).

Unlike the case of classical coding theory in the Hamming metric, the best lower bounds on $A_q(n,d)$ and $A_q(n,k,k)$ result from code constructions, the subject of the next section.

4 Constructions

4.1 Lifted Rank-Metric Codes

In this section, we describe the simplest construction of asymptotically good subspace codes, which uses rank-metric codes as building blocks. This construction was first proposed in [6], and then rediscovered in [1] for the special case where the rank-metric code is a Gabidulin code. The construction was later explained in [3, 22] in the context of the subspace/injection distance. The latter description is reviewed below.

For a matrix $X \in \mathbb{F}_q^{k\times m}$, let the subspace $\Lambda(X) \triangleq \langle [I_{k\times k}\ X] \rangle \in \mathcal{G}_q(k+m,k)$ be called the *lifting* of X. Similarly, for a matrix code $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$, let the subspace code $\Lambda(\mathcal{C}) \triangleq \{\Lambda(X),\ X \in \mathcal{C}\}$ be called the *lifting* of $\mathcal{C}$. Since every subspace corresponds to a unique matrix in RREF, we have that the mapping $X \to \Lambda(X)$ is injective, and therefore $|\Lambda(\mathcal{C})| = |\mathcal{C}|$. Note that $\Lambda(\mathcal{C})$ is a constant-dimension code, i.e., $\Lambda(\mathcal{C}) \subseteq \mathcal{G}_q(k+m,k)$.

Lemma 2 (Lifting Lemma [3]). *For all $X, X' \in \mathbb{F}_q^{k\times m}$ and all $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$,*

$$\begin{aligned} \mathsf{d}(\Lambda(X), \Lambda(X')) &= \mathsf{d}_{\mathrm{R}}(X, X'), \\ \mathsf{d}(\Lambda(\mathcal{C})) &= \mathsf{d}_{\mathrm{R}}(\mathcal{C}). \end{aligned}$$

Proof. We have

$$\begin{aligned} \mathsf{d}(\Lambda(X), \Lambda(X')) &= \mathsf{dim}(\Lambda(X) + \Lambda(X')) - \mathsf{min}\{\mathsf{dim}(\Lambda(X)),\, \mathsf{dim}(\Lambda(X'))\} \\ &= \mathsf{rank} \begin{bmatrix} I & X \\ I & X' \end{bmatrix} - k \\ &= \mathsf{rank} \begin{bmatrix} I & X \\ 0 & X' - X \end{bmatrix} - k \\ &= \mathsf{rank}(X' - X). \end{aligned}$$

The second statement immediately follows from the first.

Lemma 2 shows that a subspace code constructed by lifting inherits the distance properties of its underlying rank-metric code.

In particular, let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$ be an MRD code with $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$ and, without loss of generality, let $k \leq n - k$. Then $\Lambda(\mathcal{C})$ is an (n, d, k) code with cardinality

$$|\Lambda(\mathcal{C})| = q^{(n-k)(k-d+1)}. \tag{14}$$

Note that (14) gives a lower bound on $A_q(n, d, k)$. Comparing with the upper bound of (8), we see that the ratio of the upper and lower bounds is a constant depending only on q, thus demonstrating that this construction yields asymptotically optimal codes.

Optimizing k in (14), we obtain

$$A_q(n, d) \geq q^{\lceil \frac{n}{2} \rceil (\lfloor \frac{n}{2} \rfloor - d + 1)}.$$

We now mention a particular way of constructing lifted rank-metric codes. When $m \geq 2k$ it is convenient to construct an MRD code $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$ as a Cartesian product of simpler MRD codes. Let $m_1, \ldots, m_r \geq k$ be such that $\sum_{i=1}^r m_i = m$, and let $\mathcal{C}_i \subseteq \mathbb{F}_q^{k\times m_i}$, $i = 1, \ldots, r$, be MRD codes with minimum rank distance d. Then, it is easy to see that the Cartesian product $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_r$ is also an MRD code with $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$, where a specific element $(X_1, \ldots, X_r)$ in the Cartesian product is interpreted as the $k \times m$ matrix $[X_1\ X_2\ \cdots\ X_r]$. Clearly, we have $|\mathcal{C}| = \prod_{i=1}^r q^{m_i(k-d+1)} = q^{m(k-d+1)}$. Note the importance of choosing $m_i \geq k$ for the resulting code to be MRD. Now, since $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$, it follows that $\Lambda(\mathcal{C})$ is a $(k + m, k, d)_q$ code.

4.2 Padded Codes

Padded codes are a set of subspace codes in $\mathcal{G}_q(n,k)$ obtained as a union of lifted product rank-metric codes. Let $n=(r+1)k+s$, where $r,s\in\mathbb{N}$ and $s<k$. Let $\mathcal{C}\subseteq\mathbb{F}_q^{k\times k}$, and $\mathcal{C}'\subseteq\mathbb{F}_q^{k\times(k+s)}$ be rank-metric codes of minimum rank-distance d. Define a padded code as $\mathit{\Omega}=\bigcup_{i=0}^{r-1}\mathit{\Omega}_i$, where

$$\mathit{\Omega}_i=\{\langle[\overbrace{\mathbf{0}_{k\times k}\cdots\mathbf{0}_{k\times k}}^{i}\ I_{k\times k}\ c_{i+1}\cdots c_r]\rangle\}$$

with $c_j\in\mathcal{C}$ for $j=1,\cdots r-1$, and $c_r\in\mathcal{C}'$.

It is clear that $\mathsf{d}(\mathit{\Omega}_i)=d$. Now, let $j<i\leq r-1$, and consider $U=\langle X\rangle\in\mathit{\Omega}_i$ and $V=\langle Y\rangle\in\mathit{\Omega}_j$, where $X=[\overbrace{\mathbf{0}_{k\times k}\cdots\mathbf{0}_{k\times k}}^{i}\ I_{k\times k}\ c_{i+1}\cdots c_r]$ and $Y=[\overbrace{\mathbf{0}_{k\times k}\cdots\mathbf{0}_{k\times k}}^{j}\ I_{k\times k}\ c_{i+1}\cdots c_r]$. Since $j<i$, $I_{k\times k}$ in X and Y are not aligned. Therefore,

$$\mathsf{dim}(U+V)=\mathsf{rank}\begin{bmatrix}X\\Y\end{bmatrix}=2k,$$

and $\mathsf{d}(U,V)=\mathsf{dim}(U+V)-k=k\geq d$. Thus we obtain $\mathsf{d}(\mathit{\Omega})=d$.

When $\mathcal{C}=\mathcal{C}'$ are Gabidulin codes, we obtain a special case of the construction in [23]. If in addition $\mathsf{d}_{\mathrm{R}}(\mathcal{C})=k$, then the construction above results in the "spread codes" of [24] and [25].

4.3 Lifted FD Codes

In [26], Etzion and Silberstein provide a multi-level construction for codes in $\mathcal{P}_q(n)$. The basic idea of this construction is to generalize the lifting construction to Schubert cells (as defined in Section 2) so that a lifted rank-metric code is contained completely within any given cell. A code can then be constructed by taking a union of such lifted rank-metric codes in suitably well-separated Schubert cells. We now give a detailed description of this construction.

For a subspace $V\in\mathcal{P}_q(n)$ and a nonsingular matrix $T\in\mathbb{F}_q^{n\times n}$, define $VT\triangleq\{vT,\ v\in V\}$ (which is a subspace isomorphic to V). Given any binary vector b of length n and weight k, define $P(b)$ as the $n\times n$ permutation matrix such that $P(b)_{\mathsf{supp}(b)}=\left[I_{k\times k}\ \mathbf{0}_{k\times(n-k)}\right]$ and $P(b)_{\mathsf{supp}(\bar{b})}=\left[\mathbf{0}_{(n-k)\times k}\ I_{(n-k)\times(n-k)}\right]$. Multiplication of a matrix $\left[X\ Y\right]$, where X is

$k \times k$ and Y is $k \times (n-k)$, by $P(b)^{-1}$ on the right results in a matrix in which the columns are permuted. Specifically, the columns of X appear in columns indexed by $\mathsf{supp}(b)$, and columns of Y appear in columns indexed by $\mathsf{supp}(\bar{b})$, and the order of the columns within each submatrix is preserved.

Now, let b be a binary vector of length n and weight k. For a matrix $X \in \mathbb{F}_q^{k\times(n-k)}$, define the generalized lifting, $\Lambda_b(X)$, of X with respect to b as

$$\Lambda_b(X) \triangleq \Lambda(X)P(b)^{-1} = \left\langle \left[I \ X\right] P(b)^{-1} \right\rangle .$$

Since $\mathsf{rank}\left(\left[I \ X\right] P(b)^{-1}\right) = k$, we observe that $\Lambda_b(X)$ is a k-dimensional subspace of $\mathbb{F}_q^n$. Similarly, for a matrix code $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$, let

$$\Lambda_b(\mathcal{C}) \triangleq \{\Lambda_b(c),\, c \in \mathcal{C}\}.$$

Note that the lifting $\Lambda(\cdot)$ defined in Section 4.1 is a special case of $\Lambda_b(\cdot)$, namely, $\Lambda(X) = \Lambda_b(X)$ where $b = (1, \ldots, 1, 0, \ldots, 0)$.

The generalized lifting of a matrix code does not generally lead to a subspace code confined to a single Schubert cell. However, if the matrix code is suitably constrained in a manner depending on b, then its image will indeed be confined to the Schubert cell $\mathcal{S}_q(b)$ corresponding to b. The particular constraints are described as follows.

Let $Q = [Q_{ij}]$ be the $n \times n$ upper triangular matrix with $Q_{ij} = 1$ if $j \geq i$ and $Q_{ij} = 0$ otherwise. Given a binary profile vector b of length n and weight k, regarded as an element of $\mathbb{Z}^{1\times n}$, define the vector $c(b) \in \mathbb{Z}^{1\times n}$ via

$$c(b) \triangleq bQP(b).$$

Then, the generalized lifting $\Lambda_b(X)$ of a matrix $X = [x_{ij}] \in \mathbb{F}_q^{k\times(n-k)}$ is guaranteed to be in the Schubert cell corresponding to b provided that

$$\text{for } \ 1 \leq i \leq k,\ 1 \leq j \leq n-k,\ i > c(b)_{j+k} \text{ implies that } x_{ij} = 0. \tag{15}$$

For example, suppose $n = 8$ and $k = 3$, and let $b = (0, 0, 1, 0, 1, 0, 0, 1)$. Then,

$$P(b) = \begin{bmatrix} 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0 \end{bmatrix} \text{ and } c(b) = (1, 2, 3, 0, 0, 1, 2, 2).$$

Let $X \in \mathbb{F}_q^{3\times 5} = [x_{ij}]$. Observe that

$$\begin{bmatrix} I \ X \end{bmatrix} P(b)^{-1} = \begin{bmatrix} x_{11} & x_{12} & 1 & x_{13} & 0 & x_{14} & x_{15} & 0 \\ x_{21} & x_{22} & 0 & x_{23} & 1 & x_{24} & x_{25} & 0 \\ x_{31} & x_{32} & 0 & x_{33} & 0 & x_{34} & x_{35} & 1 \end{bmatrix}.$$

Clearly this matrix is in RREF and hence $\mathsf{prof}(\begin{bmatrix} I \ X \end{bmatrix} P(b)^{-1}) = b$ if

$$x_{11} = x_{21} = x_{31} = x_{12} = x_{22} = x_{32} = x_{23} = x_{33} = x_{34} = x_{35} = 0.$$

These conditions are precisely those implied by (15).

Now let b be a binary vector of length n and weight k. Let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$ be a rank-metric code with $\mathsf{d}_{\mathrm{R}}(\mathcal{C}) = d$ in which each codeword satisfies (15). We refer to such a code as an FD(b) code, where FD stands for "Ferrers' Diagram" [26]. Clearly, $\Lambda_b(\mathcal{C})$ consists of subspaces in the Schubert-cell corresponding to b, and by Lemma 2 we have that $\mathsf{d}(\Lambda_b(\mathcal{C})) = d$, and $\mathsf{d}_{\mathrm{S}}(\Lambda_b(\mathcal{C})) = 2d$. The code $\Lambda_b(\mathcal{C})$ is referred to as a lifted FD(b) code.

In [20, 27] a construction for FD(b) codes is presented, where a code $\mathcal{C}_b$ is obtained as a subcode of a linear MRD code with a further set of linear constraints ensuring that each codeword in $\mathcal{C}_b$ satisfies (15). The following theorem gives a lower bound on the cardinality of these codes.

Theorem 14 ([20, 27]). *For a binary vector b of length n with $\mathsf{wt}(b) = k > 0$, let $\mathcal{C}_b$ be an FD(b) code of minimum rank-distance d, obtained via the construction presented in [20, 27]. We have*

$$|\mathcal{C}_b| \geq q^{w(b) - \mathsf{max}\{\mu(b), \eta(b)\}(d-1)},$$

where $w(b) = \sum_{i>k} c(b)_i$, $\mu(b) = \mathsf{max}\{c(b)_i : i > k\}$ and $\eta(b) = \mathsf{wt}(c(b)) - k$.

We now consider the minimum distance between elements in distinct Schubert cells. Let u and v be two distinct binary vectors of length n and having weights k and k' respectively, and let $u \wedge v$ denote the logical AND of u and v, i.e., the binary vector in which $(u \wedge v)_i = u_i v_i$. Let U and V be arbitrary vector spaces in the Schubert cells $\mathcal{S}_q(u)$ and $\mathcal{S}_q(v)$, respectively. The following lower bound on $\mathsf{d}(U, V)$ is given in [20]:

Theorem 15 ([20]). $\mathsf{d}(U, V) \geq \mathsf{d}_{\mathrm{a}}(u, v)$, *where* $\mathsf{d}_{\mathrm{a}}(u, v) = \mathsf{max}\{\mathsf{wt}(u), \mathsf{wt}(v)\} - \mathsf{wt}(u \wedge v)$ *is a metric known as the asymmetric distance between u and v.*

Proof. Clearly $\mathsf{dim}(U) = \mathsf{wt}(u)$ and $\mathsf{dim}(V) = \mathsf{wt}(v)$. Let $w = u \wedge v$ and observe that $\mathsf{dim}(U \cap V) \leq \mathsf{wt}(w)$. Thus,

$$\mathsf{dim}(U) - \mathsf{dim}(U \cap V) \geq \mathsf{wt}(u) - \mathsf{wt}(w).$$

Similarly,

$$\mathsf{dim}(V) - \mathsf{dim}(U \cap V) \geq \mathsf{wt}(v) - \mathsf{wt}(w).$$

Taking the $\mathsf{max}\{\cdot, \cdot\}$ of both equations we obtain

$$\begin{aligned} \mathsf{d}(U, V) &\geq \mathsf{max}\{\mathsf{wt}(u), \mathsf{wt}(v)\} - \mathsf{wt}(w) \\ &= \mathsf{d}_{\mathrm{a}}(u, v). \end{aligned}$$

Earlier, Etzion and Silberstein [26] had given the following theorem:

Theorem 16 ([26]). $\mathsf{d}_{\mathrm{S}}(U, V) \geq \mathsf{d}_{\mathrm{H}}(u, v)$

Proof. Let $N(u, v) = \mathsf{wt}(u) - \mathsf{wt}(v)$, and $N(v, u) = \mathsf{wt}(v) - \mathsf{wt}(u)$. In a manner similar to the proof of Theorem 15 we have,

$$\begin{aligned} N(u, v) &= \mathsf{wt}(u) - \mathsf{wt}(w) \\ &= \mathsf{dim}(U) - \mathsf{wt}(w) \\ &\leq \mathsf{dim}(U) - \mathsf{dim}(U \cap V) \end{aligned}$$

Similarly $N(v, u) \leq \mathsf{dim}(V) - \mathsf{dim}(U \cap V)$, thus we have

$$d_H(u, v) = N(u, v) + N(v, u) \leq \mathsf{dim}(U) + \mathsf{dim}(V) - 2\,\mathsf{dim}(U \cap V) = \mathsf{d}_{\mathrm{S}}(U, V).$$

Note that both lower bounds are achieved with equality when U and V correspond to lifted all-zero codewords.

Finally let $\mathcal{A}$ be a binary code of length n. For every element $b \in \mathcal{A}$, let $\mathcal{C}_b$ be a FD(b) code. Then

$$\Omega = \bigcup_{b \in \mathcal{A}} \Lambda_b(\mathcal{C}_b)$$

is a subspace code.

If $\mathcal{A}$ has minimum asymmetric distance d and each FD(b) code is designed to have minimum rank-distance d, then Ω is guaranteed to have minimum injection distance d. Similarly, if $\mathcal{A}$ has minimum Hamming distance $2d$ and each FD(b) code is designed to have minimum rank-distance d, then Ω is guaranteed to have minimum subspace distance $2d$. These codes are the lifted Ferrer's diagram rank-metric codes of [20, 26] designed for the injection and subspace distance respectively. We refer to such codes as lifted FD codes.

It is interesting to observe that this construction included the padded codes of Section 4.2 as a special case. In particular, let $\mathcal{P} \subseteq \{0,1\}^n$ be a set of constant-weight binary vectors of weight $k \leq n$ such that,

$$\text{for all } v \in \mathcal{P},\ v = (\overbrace{0,0,\cdots,0}^{i}\overbrace{1,1,\cdots,1}^{k}\overbrace{0,0,\cdots,0}^{n-k-i}).$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times k}$ be a rank-metric code of minimum rank-distance d. Then $\{\Lambda_v(\mathcal{C}) : v \in \mathcal{P}\}$ is a padded code in $\mathcal{G}_q(n,k)$ with minimum injection distance d.

Notice that in this construction a naive choice for $\mathcal{A}$ would be one with a high information rate. However, a high information rate would only result in a large number of selected Schubert cells, and does not necessarily guarantee a high overall rate for the resulting $(n,d)_q$ code. This is due to the fact that the rate of a lifted FD code depends on the rate of its underlying FD(b) codes, which in turn by Theorem 14 depend on the particular choices of b.

In [26] constant-weight lexicodes are used to select well-separated Schubert cells in the Grassmannian. In [20, 27] a scoring function is defined, which given a minimum distance d, calculates for every $b \in \{0,1\}^n$ the bound of Theorem 14. In order to construct $\mathcal{A}$, a standard greedy algorithm is used that maintains a list of available profile vectors $\mathcal{A} \subseteq \{0,1\}^n$, (with $\mathcal{A}$ initialized to $\{0,1\}^n$). At each step an available vector with the highest score is added to $\mathcal{A}$, and vectors within asymmetric distance d of b are made unavailable. The algorithm proceeds until $\mathcal{A} = \emptyset$. Results obtained from this algorithm are tabulated in [27].

4.4 Codes Obtained by Integer Linear Programming

In [28] Kohnert and Kurtz view the construction of constant-dimension subspace codes as an optimization problem involving integer variables.

Let $\mathcal{C}$ be an $(n,d,k)_q$ code so that for all $U,V \in \mathcal{C}$ we have $\mathsf{d}(U,V) = k - \mathsf{dim}(U \cap V) \geq d$. The code construction problem is equivalent to finding a set of N subspaces $\mathcal{C} = \{V_1, V_2, \cdots, V_N\} \in \mathcal{G}_q(n,k)$ such that for all $i,j \in \{1,2,\cdots N\}$, $V_i, V_j \in \mathcal{C}$, we have $\mathsf{dim}(V_i \cap V_j) \leq k - d$. This means that no pair of subspaces in $\mathcal{C}$ intersect in a $(k-d+1)$-space in $\mathcal{P}_q(n)$. Let $M \in \mathbb{F}_2^{\left[{n \atop k-d+1}\right]\times\left[{n \atop k}\right]}$ be an incidence matrix defined as follows:

$$M_{W,V} := \begin{cases} 1 \text{ if } W \subseteq V, \\ 0 \text{ otherwise.} \end{cases}$$

Let x be a binary vector of length $\begin{bmatrix} n \\ k \end{bmatrix}$. The code construction problem may be viewed as the following optimization problem:

$$\text{maximize} \sum_{i=1}^{\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]} x_i, \ \text{subject to} \quad Mx \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} .$$

Let $\mathcal{S}$ be an ordered set obtained by taking the subspaces in $\mathcal{G}_q(n,k)$ in some arbitrary order. Then, if x is the solution to the above optimization problem, we may construct a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ of minimum distance d, by taking the subspaces in $\mathcal{S}$ indexed by $\mathsf{supp}(x)$.

It is possible to significantly reduce the size of the problem by prescribing a group of automorphisms for the code, and then using the induced symmetry to reduce the number of equations. See [28] for details.

5 Encoding and Decoding

Let $\Omega \in \mathcal{P}_q(n)$ be a subspace code with $\mathsf{d}(\Omega) = d$. Throughout this section, let $t = \lfloor (d-1)/2 \rfloor$. In this section, we consider two problems related to the use of Ω for error control in noncoherent linear network coding. The *encoding problem* is how to efficiently map an integer in $\{0, \ldots, |\Omega| - 1\}$ into a codeword of Ω (and back). The *decoding problem* is how to efficiently find a codeword of Ω that is closest (in injection distance) to a given subspace $U \in \mathcal{P}_q(n)$. More specifically, we focus on a *bounded-distance decoder*, which returns a codeword $V \in \Omega$ if V is the unique codeword that satisfies $\mathsf{d}(V, U) \leq t$ and returns a failure otherwise.

5.1 Encoding Lifted FD Codes

Let $\Omega = \bigcup\limits_{b \in \mathcal{A}} \Lambda_b(\mathcal{C}_b)$ be an $(n,d)_q$ lifted FD-code constructed as described in Section 4.3, and suppose that $\mathcal{A}$ is given $\{b_1, b_2, \ldots, b_{|\mathcal{A}|}\}$. Let $c_1 = 0$, and, for $2 \leq i \leq |\mathcal{A}|$, let $c_i = \sum_{j=1}^{i-1} |\mathcal{C}_{b_i}|$.

Codewords are numbered starting at zero. To map an integer m in the range $\{0, \ldots, |\Omega| - 1\}$ to a codeword: (a) find the largest index i such that $c_i \leq m$, (b) map the integer $m - i$ to a codeword of $\mathcal{C}_{b_i}$ (using an encoder for the corresponding rank-metric code), which can then be lifted to the corresponding subspace. Note that $0 \leq m_i < |\mathcal{C}_{b_i}|$. Conversely, the jth codeword of $\mathcal{C}_{b_i}$ maps back to the message $m = c_i + j$. Assuming efficient encoding of the underlying rank-metric codes, the main complexity of the encoding algorithm, given m, is to determine the corresponding c_i, which can be done using a binary search in time at worst proportional to $\log |\mathcal{A}|$.

5.2 Decoding Lifted Gabidulin Codes

Let $\mathcal{C} \subseteq \mathbb{F}_q^{k \times m}$ be a Gabidulin code with $\mathsf{d}_\mathrm{R}(\mathcal{C}) = d$. Recall that $\Lambda(\mathcal{C})$ is a $(k+m, d, k)_q$ code.

A bounded-distance decoder for $\Lambda(\mathcal{C})$ is a function $\mathsf{dec}\colon \mathcal{P}_q(n) \to \mathcal{C} \cup \{\varepsilon\}$ such that $\mathsf{dec}(U) = c$ for all $U \in \mathcal{B}_{\Lambda(c)}(t)$ and all $c \in \mathcal{C}$, and such that $\mathsf{dec}(U) = \varepsilon$ for all other U.

Let us first point out that decoding of $\Lambda(\mathcal{C})$ is not a straightforward application of rank-distance decoding. To see this, let $A \in \mathbb{F}_q^{\ell \times k}$, $y \in \mathbb{F}_q^{\ell \times (n-k)}$ and $Y = \begin{bmatrix} A \; y \end{bmatrix}$ be such that $\langle Y \rangle = U$ is the received subspace. If $\ell = k$ and A is nonsingular, then

$$\mathsf{d}(\Lambda(c), U) = \mathsf{d}_\mathrm{R}(c, A^{-1}y)$$

and therefore decoding of Ω reduces to rank-distance decoding of $\mathcal{C}$. In general, however, A may not be invertible, in which case the argument above does not hold.

Several algorithms have been proposed for implementing the function $\mathsf{dec}(\cdot)$. The first such algorithm was proposed by Kötter and Kschischang in [1] and is a version of Sudan's "list-of-1" decoding for Gabidulin codes. The time complexity of the algorithm is $O((k+m)^2 m^2)$ operations in $\mathbb{F}_q$. A faster algorithm was proposed in [3] which is a generalization of the standard ("time-domain") decoding algorithm for Gabidulin codes. The complexity of this algorithm is $O(dm^3)$ operations in $\mathbb{F}_q$. As shown in [29], the algorithm in [3] can significantly benefit from the use of optimal (or low-complexity) normal bases, further reducing the decoding complexity to $(11t^2 + 13t + m)m^2/2$ multiplications in $\mathbb{F}_q$ (and a similar number of additions). Finally, a transform-domain decoding algorithm was proposed in [22, 29], which is slightly faster than that of [3] for low-rate codes.

As we will see, a bounded-distance decoder for a lifted Gabidulin code can be used as a black box for decoding many other subspace codes. For instance, consider $\mathcal{C}^r = \mathcal{C} \times \cdots \times \mathcal{C}$, the rth Cartesian power of a Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_q^{k \times m}$. Recall that $\Lambda(\mathcal{C}^r)$ is a $(k + rm, d, k)_q$ code, where $d = \mathsf{d}_\mathrm{R}(\mathcal{C})$. Let $\mathsf{dec}(\cdot)$ be a bounded-distance decoder for $\Lambda(\mathcal{C})$. Then a bounded-distance decoder for $\Lambda(\mathcal{C}^r)$ can be obtained as the map $\mathcal{P}_q(k + rm) \to \mathcal{C}^r \cup \{\varepsilon\}$ given by

$$U \mapsto \begin{cases} \begin{bmatrix} \hat{c}_1 \cdots \hat{c}_r \end{bmatrix} = \hat{c} & \text{if } \hat{c}_i \neq \varepsilon,\ i = 1, \ldots, r, \text{ and } \mathsf{d}(\Lambda(\hat{c}), U) \leq t \\ \varepsilon & \text{otherwise} \end{cases}$$

where $\hat{c}_i = \mathsf{dec}(\langle \begin{bmatrix} A \; y_i \end{bmatrix} \rangle)$, $i = 1, \ldots, r$, and $A \in \mathbb{F}_q^{\ell \times k}$ and $y_1, \ldots, y_r \in \mathbb{F}_q^{\ell \times m}$ are such that $\langle \begin{bmatrix} A \; y_1 \cdots y_r \end{bmatrix} \rangle = U$. In other words, we can decode

$\varLambda(\mathcal{C}^r)$ by decoding each Cartesian component individually (using the same matrix A on the left) and then checking whether the resulting subspace codeword is within the bounded distance from U.

5.3 Decoding Lifted FD Codes

Let $\mathcal{A}$ be a binary code with $\mathsf{d}_\mathrm{a}(\mathcal{A}) \geq d$. For all $b \in \mathcal{A}$, let $\mathcal{C}_b$ be a b-FD code with $\mathsf{d}_\mathrm{R}(\mathcal{C}_b) \geq d$. Let

$$\varOmega = \bigcup_{b \in \mathcal{A}} \varLambda_b(\mathcal{C}_b).$$

Recall that $\varOmega$ is an $(n, d)_q$ code.

A bounded-distance decoder for $\varOmega$ is a function $\mathsf{dec}\colon \mathcal{P}_q(n) \to (\mathcal{A} \times \cup_{b \in \mathcal{B}} \mathcal{C}_b) \cup \{\varepsilon\}$ such that $\mathsf{dec}(U) = (b, c)$ for all $U \in \mathcal{B}_{\varLambda_b(c)}(t)$, all $c \in \mathcal{C}_b$, and all $b \in \mathcal{A}$, and such that $\mathsf{dec}(U) = \varepsilon$ for all other U.

We will show that we can efficiently decode $\varOmega$, provided that we have efficient decoders for $\mathcal{A}$ and for each $\mathcal{C}_b$, $b \in \mathcal{A}$. The basic procedure was proposed in [26] for the decoding in the subspace metric. Here we adapt it for the injection metric.

Let us first consider the decoding of $\varLambda_b(\mathcal{C}_b)$, for some $b \in \mathcal{A}$. Let $c \in \mathcal{C}_b$ and $U \in \mathcal{P}_q(n)$. Recall that $\varLambda_b(c) = \varLambda(c)P(b)^{-1}$. Since $P(b)$ is a nonsingular linear transformation, and therefore preserves dimensions, we have

$$\mathsf{d}(\varLambda_b(c), U) = \mathsf{d}(\varLambda_b(c)P(b), UP(b)) = \mathsf{d}(\varLambda(c), UP(b)).$$

It follows that bounded-distance decoding of $\varLambda_b(\mathcal{C}_b)$ can be performed by first computing $\hat{c} = \mathsf{dec}(UP(b))$, and then returning $(b, \hat{c})$ unless $\hat{c} = \varepsilon$.

Now, consider the decoding of $\varOmega$. Let $U \in \mathcal{P}_q(n)$ be such that $\mathsf{d}(V, U) \leq t$, for some (unique) $V \in \varOmega$. The first step is to compute the profile vector b corresponding to the Schubert cell containing V. Let b' denote the profile vector corresponding to the Schubert cell containing U. Since by Theorem 15

$$\mathsf{d}_\mathsf{a}(b, b') \leq \mathsf{d}(V, U) \leq t,$$

it follows that b can be found by inputting b' to a bounded-asymmetric-distance decoder for $\mathcal{A}$. Then the actual $c \in \mathcal{C}_b$ such that $V = \varLambda_b(c)$ can be found by using the decoder for $\mathcal{C}_b$ described above.

6 Conclusions and Open Questions

Subspace codes represent an intriguing domain in which to carry out basic investigations of coding theory.

From a practical standpoint, at least for applications in network coding, the main problems appear to be solved, as constant-dimension lifted rank-metric codes contain close to the maximum possible number of codewords (at least on a logarithmic scale), and efficient encoding and decoding algorithms have been developed. It is unlikely that codes with marginally larger codebooks (even though they exist) will justify the additional complexity needed to process them.

From a mathematical standpoint, however, much remains open. For example, what are the optimal codes of minimum distance 2 or 3? Can existing constructions be improved? For example, the construction of lifted FD codes, which relies on a partitioning of $\mathcal{P}_q(n)$ into Schubert cells, can be regarded as a form of generalized concatenation. Are there other partitioning schemes that, for example, result in subsets of increasing minimum distance? Are there interesting subspace codes that can be constructed as orbits of a group action on vector spaces? Finally, are there additional applications of subspace codes beyond those of network coding and linear authentication?

References

1. Kötter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory **54**(8) (Aug. 2008) 3579–3591
2. Silva, D., Kschischang, F.R.: On metrics for error correction in network coding. IEEE Trans. Inf. Theory (2009) to appear.
3. Silva, D., Kschischang, F.R., Kötter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory **54**(9) (2008) 3951–3967
4. Silva, D., Kschischang, F.R.: Universal secure network coding via rank-metric codes. IEEE Trans. Inf. Theory (2008) submitted for publication.
5. Katti, S., Katabi, D., Balakrishnan, H., Médard, M.: Symbol-level network coding for wireless mesh networks. In: ACM SIGCOMM, Seattle, WA (August 2008)
6. Wang, H., Xing, C., Safavi-Naini, R.: Linear authentication codes: bounds and constructions. IEEE Trans. Inf. Theory **49**(4) (2003) 866–872
7. Xia, S.T., Fu, F.W.: Johnson type bounds on constant dimension codes. Designs, Codes and Cryptography **50**(2) (February 2009) 163–172
8. Borel, A.: Linear Algebraic Groups. Second edn. Number 126 in Grad. Texts Math. Springer (1991)
9. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs. Springer Verlag, New York, NY (1989)
10. van Lint, J.H., Wilson, R.M.: A Course in Combinatorics. Second edn. Cambridge University Press, Cambridge, UK (2001)

11. Gabidulin, E.M.: Theory of codes with maximum rank distance. Probl. Inform. Transm. **21**(1) (1985) 1–12
12. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. J. of Comb. Theory. Series A **25** (1978) 226–241
13. Loidreau, P.: Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs. Ph.d. dissertation, École Polytechnique, Paris, France (May 2001)
14. Gadouleau, M., Yan, Z.: Packing and covering properties of cdcs and subspace codes. Submitted to *IEEE Trans. on Inform. Theory* (2008)
15. Delsarte, P.: An algebraic approach to association schemes of coding theory. Philips J. Res. (1973) 1–97
16. Frankl, P., Wilson, R.: The Erdös-Ko-Rado Theorem for Vector Spaces. Journal of Combinatorial Theory **43** (1986) 228–236
17. Etzion, T., Vardy, A.: Error-correcting codes in projective space. In: Proc. IEEE Int. Symp. Information Theory, Toronto, Canada (July 6–11 2008) 871–875
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam, The Netherlands (1977)
19. Ahlswede, R., Aydinian, H.: On error control for random network coding. In: IEEE Workshop on Network Coding, Theory and Applications. (2009)
20. Khaleghi, A., Kschischang, F.R.: Projective space codes for the injection metric. In: Proc. 11th Canadian Workshop Inform. Theory, Ottawa, Canada (May 13–15 2009) 9–12
21. Tolhuizen, L.M.G.M.: The generalized Gilbert-Varshamov bound is implied by Túran's theorem. IEEE Trans. Inf. Theory **43**(5) (September 1997) 1605–1606
22. Silva, D.: Error Control for Network Coding. PhD thesis, University of Toronto, Toronto, Canada (2009)
23. Skachek, V.: Recursive code construction for random networks. Submitted for Publication (2008)
24. Manganiello, F., Gorla, E., Rosenthal, J.: Spread codes and spread decoding in network coding. In: Proc. IEEE Int. Symp. Information Theory, Toronto, Canada (July 6–11 2008) 881–885
25. Gabidulin, E., Bossert, M.: Codes for network coding. In: Proc. IEEE Int. Symp. Information Theory, Toronto, Canada (July 6–11 2008) 867–870
26. Etzion, T., Silberstein, N.: Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. IEEE Trans. Inf. Theory **55**(7) (July 2009) 2909–2919
27. Khaleghi, A.: Projective space codes for the injection metric. Master's thesis, University of Toronto, Toronto, Canada (2009)
28. Kohnert, A., Kurz, S.: Construction of large constant dimension codes with a prescribed minimum distance. Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth (2008) 31–42
29. Silva, D., Kschischang, F.R.: Fast encoding and decoding of Gabidulin codes. In: Proc. IEEE Int. Symp. Information Theory, Seoul, Korea (June 28–July 3 2009) 2858–2862