On error control codes for random network coding

R. Ahlswede and H. Aydinian
Department of Mathematics
University of Bielefeld
POB 100131, D-33501
Bielefeld, Germany
Email: (ahlswede),(ayd)@math.uni-bielefeld.de

***Abstract*—The random network coding approach is an effective technique for linear network coding, however it is highly susceptible to errors and adversarial attacks. Recently Kötter and Kschischang [14] introduced the operator channel, where the inputs and outputs are subspaces of a given vector space, showing that this is a natural transmission model in noncoherent random network coding. A suitable metric, defined for subspaces: $d_S(U,V) = \dim U + \dim V - 2\dim(U \cap V)$, gives rise to the notion of codes capable of correcting different kinds of errors (like packet errors, erasures etc.) in noncoherent random network coding. In this paper we continue the study of coding for operator channels started in [14]. We consider codes correcting insertions/deletions (dimension enlargement and dimension reduction respectively). Bounds and constructions for those codes are presented.**

I. Introduction

Network coding, since its beginning [2], proposes us new (challenging) theoretical and algorithmic problems. Recently Kötter and Kschischang [14] developed a novel framework for random network coding [11], introducing a new class of error-control coding problems related to coding over networks. Random network coding has shown [5], [11], [12] to be a powerful technique for disseminating information in networks, in particular for multicast communication, with unknown (or changing) topology. It is known, however, that (random) network coding is highly susceptible to packet transmission errors (caused by various sources) like noise, malicious or mulfunctioning nodes, or insufficient min-cut. Thus for practical application error control in network coding is an important problem.

Error correction in network coding was originally introduced and studied by Cai and Yeung [4], [21] (see also [22]). Their approach (called coherent network coding) is based on the knowledge of the network topology and considered the design of a network code as part of the error control problem. An alternative approach introduced by Kötter and Kschischang [14] (called noncoherent network coding), is that source and destination nodes have no knowledge about network topology.

In the basic transmission model the network operates with packets of length m considered as vectors over a given finite field. The source node injects n packets in the network, which propagate through the network. Each intermediate node in the network creates a random linear combination of packets, it has received, and transmits this linear combination. Finally, the receiver collects N such randomly generated (and possibly corrupted) packets and tries to infer the packets injected into the network. Note that the number of received packets is not predetermined (the receiver collects as many packets as possible). In an adversarial model of transmission (see [14]) it is assumed that the adversaries have access to some intermediate nodes with the ability to inject erroneous packets, adding them additively to the packets produced by the nodes. The matrix form of the transmission model is described as follows. Let X be an $n \times m$ matrix whose rows correspond to n transmitted packets of the source and let Y be an $N \times m$ matrix with rows corresponding to the received packets of length m. Then

$$Y = HX + GE, \tag{I.1}$$

where E is an $t \times m$ error matrix, H and G are random $N \times n$ and $N \times t$ martices, respectively.

In [14] Kötter and Kschischang define the *subspace channel* (or *operator channel*) as a discrete memoryless channel where the inputs and outputs are subspaces of a given vector space. The goal of the receiver is to reconstruct the subspace sent by the transmitter in the presence of different kinds of errors (introduced adversarially) like packet errors, erasures etc.

Let $GF(q)^n$ be a vector space over the Galois field $GF(q)$. The set of all subspaces of $GF(q)^n$, called projective space, is denoted by $\mathcal{P}_q(n)$. Given an integer $0 \leq k \leq n$, the set of all k-subspaces (k-dimensional subspaces) of $GF(q)^n$ is called a *Grassmannian* and

978-1-4244-4724-4/09/$25.00 © 2009 IEEE

denoted by $\mathcal{G}_q(n,k)$. Thus we have $\bigcup_{0\le k\le n}\mathcal{G}_q(n,k)=\mathcal{P}_q(n)$. It is known that the size of the Grassmannian $|\mathcal{G}_q(n,k)|=|\mathcal{G}_q(n,n-k)|$ $(k=0,1,\dots,n)$ is determined by the q-ary Gaussian coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \triangleq \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}. \quad \text{(I.2)}$$

A natural measure of nearness in $\mathcal{P}_q(n)$ is the distance function d_S defined for all subspaces $U,V\in\mathcal{P}_q(n)$ by

$$d_S(U,V)=\dim U+\dim V-2\dim(U\cap V). \quad \text{(I.3)}$$

It is known that d_S is a metric and thus $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$ are metric spaces. A code $\mathcal{C}$ in $\mathcal{P}_q(n)$ is a nonempty subset in it. The minimum distance $d_S(\mathcal{C})$ of a code $\mathcal{C}$ is the minimum of $d_S(X,Y)$ taken over all distinct elements $X,Y\in\mathcal{C}$. For the ground space $GF(q)^n$ we call n the code length. We say then that $\mathcal{C}$ is an $(n,d)_q$–code if $d_S(\mathcal{C})\ge d$. Similarly, when $\mathcal{C}\subset\mathcal{G}_q(n,k)$, we speak about a constant dimension $(n,d,k)_q$–code.

In [14] Kötter and Kschischang showed that subspace codes with minimum distance $d_S>2t+2e$ are capable of correcting any t packet errors and e erasures (dimension reduction).

We denote by $A_q(n,d)$ the maximum size of a code $\mathcal{C}\subseteq\mathcal{P}_q(n)$ with $d_S(\mathcal{C})=d$. Similarly we use the notation $A_q(n,2r,k)$ for the maximum size of a constant dimension code $\mathcal{C}\subseteq\mathcal{G}_q(n,k)$ with $d_S(\mathcal{C})=2r$. The sum of two subspaces U,V is defined as

$$U+V\triangleq\{u+v: u\in U, v\in V\}=\text{span}(U\cup V).$$

The paper is organized as follows. In Section II our main observation is that bounds of code sizes for the operator channel can easily be derived by our approach in [1]. In its more general form hinted at already in [1], it takes the form of Lemma 1 with Corollary 1. We demonstrate this by first giving short proofs of recently established Singleton like (Theorem 1) and Johnson like (Theorem 2) bounds. However, our approach goes further, in fact we obtain the sharper upper bound of Theorem 3. Finally, a Varshamov-Gilbert like bound of Etzion and Vardy is included as Theorem 4 for comparison. In Section III we define a distance (metric) which is suitable for correction of insertions/deletions for operator channels. We show that the size of a code in $P_q(n)$ capable of correcting t insertions/deletions cannot exceed more than $t+1$ times the size of a code with minimum distance $d_S=2t+1$ (Theorem 5). We also establish a linear programming bound on the size of codes correcting a given number of insertions/deletions (Theorem 6). Finally, the problem of error detection is considered and the maximum size of a code capable of detecting a given number of insertions/deletions is determined (Theorem 7). In Section IV we give a construction of codes correcting single insertions/deletions for operator channels (Theorem 8).

II. Bounds on the size of codes

Most studies on codes in $\mathcal{P}_q(n)$ are related to codes in Grassmannians. The graph associated with $\mathcal{G}_q(n,k)$ is called the Grassmann graph and we denote it in the same way. There is a certain similarity between Grassmann graphs and Johnson graphs (see [3] for definitions). Both have strong regularities : they are distance-regular and distance-transitive ([3]). Note however that the graph associated with $\mathcal{P}_q(n)$ is not even regular.

We start with a general bound for codes on transitive graphs, which can be applied to derive bounds for codes in Grassmannians.

Lemma 1: Let $\Gamma=(\mathcal{V},\mathcal{E})$ be a graph that admits a transitive group of automorphisms $Aut(\Gamma)$ and let A,B be arbitrary subsets of the vertex set $\mathcal{V}$. Then there exists $g\in Aut(\Gamma)$ such that

$$\frac{|g(A)\cap B|}{|B|}\ge\frac{|A|}{|\mathcal{V}|}. \quad \text{(II.1)}$$

Proof: The statement is easy to prove by counting the number of all pairs $(a,g)\in A\times Aut(\Gamma)$, such that $g(a)\in B$, in two ways (then using the transitivity and the well-known orbit-stabilizer Theorem). ■

The inequality II.1 can be viewed as a generalization of Delsarte's anticode bound [6] stated for distance-regular graphs (association schemes), in particular for Grassmann graphs. The graph $\mathcal{G}_q(n,k)$ has a distance-transitive group of authomorphisms $PGL(n,q)$ (projective linear group), thus we can apply here Lemma 1, which in particular gives the following

Corollary 1: [1] Let $\mathcal{C}_D\subseteq\mathcal{G}_q(n,k)$ be a code with distances from $D=\{d_1,\dots,d_s\}\subseteq\{1,\dots,n\}$. Then for an arbitrary 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

$$\frac{|\mathcal{C}_D^*(\mathcal{B})|}{|\mathcal{B}|}\ge\frac{|\mathcal{C}_D|}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \quad \text{(II.2)}$$

In case $\mathcal{C}$ is an $(n,d,k)_q$– code and $\mathcal{B}$ is an anticode with diameter $d-1$ (and hence $|\mathcal{C}_{d-1}^*(\mathcal{B})|=1$) we have Delsarte's anticode bound

$$|\mathcal{C}|\le\frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{|\mathcal{B}|}. \quad \text{(II.3)}$$

Let us mention another important (from the coding theory point of view) class of transitive graphs. Let $\mathbb{F}_q^{n\times m}$ denote the set of all $n\times m$ matrices over $GF(q)$. The rank-distance between $X,Y\in\mathbb{F}_q^{n\times m}$ is defined as $d_R(X,Y)=\text{rank}(X-Y)$. It is known that the rank-distance is a metric [6], [10]. The graph associated with $\mathbb{F}_q^{n\times m}$ is distance-transitive (see [3]). Codes in space $\mathbb{F}_q^{n\times m}$ with rank metric d_R are called rank-metric codes. Rank-metric codes are introduced by Delsarte [6] and studied by Gabidulin [10]. In fact, Lemma 1 and Corollary 1 (applied for rank-metric codes) hold for metric spaces $(\mathbb{F}_q^{n\times m}, d_R)$.

Next we mention known bounds for constant dimension codes. Let $\mathcal{B}_t$ be a ball of radius t in $\mathcal{G}_q(n,k)$. The size of $\mathcal{B}_t$ depends only on its radius and equals $\sum_{i=0}^{t}\begin{bmatrix}k\\i\end{bmatrix}_q\begin{bmatrix}n-k\\i\end{bmatrix}_q q^{i^2}$ (see [3], [14]). Taking $t=\lfloor (r-1)/2\rfloor$ one has the following sphere packing bound established in [14]

$$A_q(n,2r,k)\le\frac{|\mathcal{G}_q(n,k)|}{|\mathcal{B}_t|}=\frac{\begin{bmatrix}n\\k\end{bmatrix}_q}{\sum_{i=0}^{t}\begin{bmatrix}k\\i\end{bmatrix}_q\begin{bmatrix}n-k\\i\end{bmatrix}_q q^{i^2}}. \tag{II.4}$$

Note that $\mathcal{B}_t$ (with $t=\lfloor (r-1)/2\rfloor$) is an anticode of diameter $2r-2$.

Kötter and Kschischang proved the following

Theorem 1: [14] (Singleton like bound)

$$A_q(n,2r,k)\le\begin{bmatrix}n-r+1\\k-r+1\end{bmatrix}_q. \tag{II.5}$$

The next bound (mentioned in [19], [8]) follows directly from Delsarte's anticode bound, taking as an anticode of diameter $2r-2$ all k–spaces (in $\mathcal{P}_q(n)$) containing a fixed $(k-r+1)$– space, thus having the cardinality $\begin{bmatrix}n-k+r-1\\r-1\end{bmatrix}_q$. Frankl and Wilson [9] showed that for all integers $n\ge 2k$ this is the maximum possible size of an anticode of diameter $2r-2$. Thus we have the following (anticode bound)

$$A_q(n,2r,k)\le\frac{\begin{bmatrix}n\\k\end{bmatrix}_q}{\begin{bmatrix}n-k+r-1\\r-1\end{bmatrix}_q}=\frac{\begin{bmatrix}n\\k-r+1\end{bmatrix}_q}{\begin{bmatrix}k\\k-r+1\end{bmatrix}_q}. \tag{II.6}$$

Note that the last bound implies nonexistence of nontrivial constant dimension perfect codes, since the size of an optimal anticode is always greater than the size of a ball of the same diameter. The bound II.6 also follows from the notion of Steiner structures in Grassmann graphs. A set $S\subseteq\mathcal{G}_q(n,k)$ is called a $(t,k,n)_q$–Steiner structure if each t-space in $\mathcal{P}_q(n)$ is contained in precisely one k–space of S. Every $(k-r+1,k,n)_q$– Steiner structure in $\mathcal{G}_q(n,k)$ is an $(n,2r,k)_q$– perfect diameter code (code attaining the anticode bound) in $\mathcal{G}_q(n,k)$ and vice versa (see [1]). Note however, that no nontrivial Steiner structures, except for spreads of $\mathcal{P}_q(n)$ by k–spaces (in case when $k|n$), are known. Properties of Steiner structures in Grassmann graphs are studied in [17].

The bound II.6 is shown to be always better [20] than the bound II.5.

The next bounds are the counterparts of the well known Johnson bounds (see [16]) for constant weight codes.

Theorem 2: [8], [20] (Johnson like bounds)

$$A_q(n,2r,k)\le\lfloor\frac{q^n-1}{q^k-1}\mathcal{A}_q(n-1,2r,k-1)\rfloor \tag{II.7}$$

$$A_q(n,2r,k)\le\lfloor\frac{q^n-1}{q^{n-k}-1}A_q(n-1,2r,k)\rfloor. \tag{II.8}$$

Iterating II.7 one gets the following bound ([8], [20])

$$A_q(n,2r,k)=\lfloor\frac{q^n-1}{q^k-1}\lfloor\frac{q^{n-1}-1}{q^{k-1}-1}\dots\lfloor\frac{q^{n-k+r}-1}{q^r-1}\rfloor\dots\rfloor\rfloor, \tag{II.9}$$

which in fact is an improvement of II.5 (since it gives the RHS of II.5 with brackets removed).

We note that both inequalities in II.6 can be easily derived from II.2. Indeed, if we take as a subset $\mathcal{B}\subseteq\mathcal{G}_q(n,k)$ (in II.2), the set of all k–spaces contained in a fixed $(n-1)$–space $H\in\mathcal{P}_q(n)$ (thus $|\mathcal{B}|=\begin{bmatrix}n-1\\k\end{bmatrix}$), we get inequality II.8. Similarly, for a fixed vector $v\notin H$, and $\mathcal{B}$ defined as
$\mathcal{B}=\{(V+v)\in\mathcal{G}_q(n,k): V\in\mathcal{G}_q(n,k-1), V\subset H\}$, (thus $|\mathcal{B}|=\begin{bmatrix}n-1\\k-1\end{bmatrix}$), we get inequality II.7.

Let us give another upper bound, derived from the inequality II.2, by choosing a subset $\mathcal{B}$ in a suitable way.

Theorem 3: For integers $0\le t\le r\le k$, $k-t\le m\le n$ we have

$$A_q(n,2r,k)\le\frac{\begin{bmatrix}n\\k\end{bmatrix}_q A_q(m,2r-2t,k-t)}{\sum_{i=0}^{t}q^{i(m-i)}\begin{bmatrix}m\\k-i\end{bmatrix}_q\begin{bmatrix}n-m\\i\end{bmatrix}_q}. \tag{II.10}$$

Proof: Let $W\in\mathcal{P}_q(n)$ be a fixed subspace with $\dim(W)=m$ and $t\le r$. Then we define $\mathcal{B}=\{U\in\mathcal{G}_q(n,k):\dim(U\cap W)\ge k-t\}$. One can observe that $|\mathcal{B}|=\sum_{i=0}^{t}q^{i(m-i)}\begin{bmatrix}m\\k-i\end{bmatrix}_q\begin{bmatrix}n-m\\i\end{bmatrix}_q$ and the size of a code $\mathcal{C}^*\subseteq\mathcal{B}$ of minimum distance $2r$ is upper bounded by $A(m,2r-2t,k-t)$. ■

Note that the last bound can be regarded as a sharpening of II.8, since for $t=0$ and $m=n-1$ we get bound II.8.

Etzion and Vardy [8] derived a linear programming bound for $A_q(n,d)$ and the following lower bound.

Theorem 4: [8] (Varshamov-Gilbert like bound).

$$A_q(n,d)\ge\frac{|\mathcal{P}_q(n)|^2}{\sum_{k=0}^{n}\sum_{i=0}^{d-1}\sum_{i=0}^{j}\begin{bmatrix}n-k\\j-i\end{bmatrix}_q\begin{bmatrix}k\\i\end{bmatrix}_q\begin{bmatrix}n\\k\end{bmatrix}_q q^{i(j-i)}}. \tag{II.11}$$

They also proved [8] the nonexistence of a nontrivial perfect code in $P_q(n)$, (in the sense that $\mathcal{P}_q(n)$ cannot be nontrivially partitioned into balls).

III. Operator channel with insertion/deletion: error correction and error detection

The operator channel defined in [14] gave rise to notions of deletions and insertions (dimension reduction and dimension enlargement respectively).

Definition 1: We say that a code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is capable of correcting t insertions if for every $U, V \in \mathcal{C}$ and $X, Y \in \mathcal{P}_q(n)$ with $\dim X, \dim Y \leq t$ we have

$$U + X \neq V + Y \tag{III.1}$$

For every $U, V \in \mathcal{P}_q(n)$ define

$$d_A(U, V) = \max\{\dim U, \dim V\} - \dim(U \cap V). \tag{III.2}$$

Note that

$$2d_A(U, V) = d_S(U, V) + |\dim U - \dim V|. \tag{III.3}$$

Proposition 1: A code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is capable of correcting t insertions (deletions) if and only if the minimum distance of the code $d_A(\mathcal{C}) \geq t + 1$.

Note that a code $\mathcal{C} \subseteq \mathcal{G}_q(n, k)$ capable of correcting t insertions (deletions) is an $(n, 2t+2, k)_q$–code, since for $U, V \in \mathcal{G}_q(n, k)$ (in view of III.3) holds $2d_A(U, V) = d_S(U, V)$.

Proposition 2: Given integers e, g a code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is capable of correcting up to e insertions and g deletions if and only if $d_A(\mathcal{C}) \geq t + 1$ where $t = e + g$.

Clearly, the proposition implies that all results concerning codes capable of correcting t insertions (or symmetrically t deletions) are extended to codes correcting up to a given number of e insertions and $t - e$ deletions.
The next result compairs the size of an optimal code correcting t insertions with a code of the same dimension n and minimum distance $d_S = 2t + 1$. Let $B_q(n, t)$ denote the maximum size of a code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ capable of correcting t insertions (deletions).

Theorem 5: Given integers $1 \leq t \leq n$ we have

$$A_q(n, 2t+1) \leq B_q(n, t) \leq (t+1)A_q(n, 2t+1). \tag{III.4}$$

Proof: Let $\mathcal{C}(n, t) \subset \mathcal{P}_q(n)$ be a code capable of correcting t–insertions (deletions). The simple idea of the proof is that $\mathcal{C}(n, t)$ can be partitioned into $t+1$ codes $\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_t$ each of which is a code of minimum distance $d_S \geq 2t+1$. Define first $\mathcal{D}_i = \{U \in \mathcal{C} : \dim U \equiv i \mod 2t+2\}$, for $i = 0, 1, \dots, 2t+1$. Note that each $\mathcal{D}_i$ has minimum distance $d_S \geq 2t + 2$. Moreover, it is not hard to observe that $\mathcal{D}_i \cup \mathcal{D}_{i+1}$ has minimum distance $d_S \geq 2t + 1$ (for any i). Thus taking $\mathcal{C}_i = \mathcal{D}_{2i} \cup \mathcal{D}_{2i+1}$, for $i = 0, 1 \dots, t$, we get the desired partition. ■

Next we establish an upper bound for $B_q(n, t)$.

Theorem 6: (Linear programming bound)
For integers $1 \leq t \leq n/2$, let

$$f(n, t, q) = \max(f_0 + f_1 + \dots + f_n)$$

subject to linear constraints:

$f_0, f_1, \dots, f_n$ are nonnegative integers with

$f_0 = f_n = 1,\ f_k = f_{n-k} = 0$ for $k = 1, \dots, t$,

$$f_k + \frac{1}{t+1}\sum_{i=1}^{t}(t+1-i)(f_{k-i}\begin{bmatrix} n-k+i \\ n-k \end{bmatrix}_q + f_{k+i}\begin{bmatrix} k+i \\ k \end{bmatrix}_q)$$

$\leq \begin{bmatrix} n \\ k \end{bmatrix}_q$, for $k = 0, \dots, n$,

$f_k \leq A_q(n, 2t+2, k)$, for $k = 0, \dots, n$,

$f_{-j} = f_{n+j} = 0$ for $i = 1, \dots, t$ (by convention).

Then

$$B_q(n, t) \leq f(n, t, q). \tag{III.5}$$

Proof: Let $\mathcal{C}(n, t) \subseteq \mathcal{P}_q(n)$ be a code capable of correcting t insertions (deletions) and let $A_i = |\mathcal{C}(n, t) \cap \mathcal{G}_q(n, i)|,\ i = 0, 1, \dots, n$. Observe first that $\sum_{i=0}^{t} A_i = \sum_{i=n-t-i}^{n} A_i = 1$. Moreover, we may always assume that for an optimal code we have $A_0 = A_n = 1$. Given integers $0 \leq \ell, r \leq n$ and a subspace $U \in \mathcal{P}_q(n)$, let us define $\Gamma_{\ell,r}(U) \triangleq \{V \in \mathcal{P}_q(n) : V \subseteq U,\ d_S(U, V) \leq \ell\} \bigcup \{V \in \mathcal{P}_q(n) : V \supseteq U,\ d_S(U, V) \leq r\}$. It is not hard to show that for every distinct subspaces $U, V \in \mathcal{C}(n, t)$, the sets $\Gamma_{\ell,r}(U)$ and $\Gamma_{\ell,r}(V)$ are disjoint if $\ell + r \leq t$. Then for a given integer $0 \leq \ell \leq t$, the number of k-spaces in the union $\bigcup \Gamma_{\ell,t-\ell}(V)$, taken over all elements $V \in \mathcal{C}(n, t)$, is determined by

$$\sum_{i=1}^{t-\ell} A_{k-i}\begin{bmatrix} n-k+i \\ i \end{bmatrix}_q + \sum_{i=0}^{\ell} A_{k+i}\begin{bmatrix} k+i \\ k \end{bmatrix}_q \leq \begin{bmatrix} n \\ k \end{bmatrix}_q. \tag{III.6}$$

We infer the result, summing inequalities in III.6 for $\ell = 0, 1, \dots, t$. ■

Let us also define the notion of error detection for the operator channel with insertions/deletions.

Definition 2: We say that a code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is capable of detecting t insertions (deletions) if for every $U, V \in \mathcal{C}$ and $X \in \mathcal{P}_q(n)$ with $\dim X \leq t$ we have

$$U + X \neq V. \tag{III.7}$$

Proposition 3: A code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is capable of detecting t insertions (deletions) if and only if for every

$U, V \in \mathcal{C}$ with $U \subset V$ we have

$$d_S(U,V) \geq t+1. \tag{III.8}$$

Let $D_q(n,t)$ denote the maximum size of a code capable of detecting t insertions (deletions).

Theorem 7: Given integers $1 \leq t \leq n$ we have

$$D_q(n,t) = \max_{0 \leq r \leq t} \sum_{i \equiv r \mod (t+1)} \begin{bmatrix} n \\ i \end{bmatrix}_q . \tag{III.9}$$

Proof: For the proof we use a result by Kleitman [13] for regular rank unimodal posets (the linear lattice $L(n,q)$ is regular and rank unimodal). The result applied to the linear lattice $L(n,q)$ implies that the maximum cardinality of a subset of $\mathcal{P}_q(n)$ satisfying condition III.8 is attained for the largest $\mathcal{C}_r \triangleq \{U \in P_q(n) : \dim U = r \mod (t+1)\}$, taken over all $0 \leq r \leq t$. ■

IV. Code constructions

Kötter and Kschischang [14] gave a construction of constant-dimension codes, that is codes in Grassmannians. These codes are described in [18] in terms of rank-metric codes. An important class of rank-metric codes are Gabidulin codes [10] which are maximum-rank-distance codes (MRD). It is known [10] that for a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ with minimum distance $d_R(\mathcal{C})$ one has the Singleton bound $\log_q |\mathcal{C}| \leq \min\{n(m - d_R(\mathcal{C}) + 1), m(n - d_R(\mathcal{C}) + 1)\}$. Codes attaining this bound are called maximum-rank-distance codes (MRD). Gabidulin codes are linear MRD codes, which exist for all parameters n, m and $d_R \leq \min\{n,m\}$. The construction in [14], called *lifted code*, is as follows. Given an MRD code $\mathcal{C} \subset \mathbb{F}_q^{n\times m}$ with minimum distance d_R the lifted code $\widehat{\mathcal{C}} \subseteq \mathcal{G}_q(n+m, n)$ is defined as the set of n-spaces correspoding to the rowspaces of the matrices $[I_n|A] : A \in \mathcal{C}$, where I_n is the $n\times n$ identity matrix. The lifted code $\widehat{\mathcal{C}}$ has minimum distance $d_S(\widehat{\mathcal{C}}) = 2d_R(\mathcal{C})$. The lifting construction gives asymptotically optimal codes with cardinality $|\widehat{\mathcal{C}}| \geq \frac{1}{4}A_q(n+m, 2d, n)$ (see [14]). Etzion and Silberstein [7] gave a construction of constant dimension codes using Gabidulin codes and Ferrers diagrams. Their construction improves the lifted codes in the sence that lifted codes are always subcodes of those codes. Only a few constructions of codes in $\mathcal{P}_q(n)$ are known [7], [8]. The first nontrivial (but still simple) problem is the construction of optimal codes with minimum distance $d_S = 2$. In fact, $A_q(n,2)$ is the independence number of the graph $\mathcal{P}_q(n)$. Let $\mathcal{P}_0, \mathcal{P}_1$ be the set of all subspaces in $\mathcal{P}_q(n)$ with even and odd dimensions respectively. Then Theorem 7 tells us that $A_q(n,2) = \max\{|\mathcal{P}_0|, |\mathcal{P}_1|\}$ (note that for n even $|\mathcal{P}_0| \neq |\mathcal{P}_1|$).

Our next goal is the construction of codes in $\mathcal{P}_q(n)$ capable of correcting single insertions (deletions). A simple idea is to construct such a code in $\mathcal{P}_0$ (or in $\mathcal{P}_1$): we need only to construct a constant dimension $(n, 4, 2k)_q$–code for each $k = 0, 1, \ldots, \lfloor n/2 \rfloor$. This can be done with lifted codes for each k. Let us denote this code by $\widehat{\mathcal{C}}_0$ (respectively by $\widehat{\mathcal{C}}_1$ for the code in $\mathcal{P}_1$). Note that $d_S(\widehat{\mathcal{C}}_0) = d_A(\widehat{\mathcal{C}}_0) = 2$. However one can do better. We construct a code $\mathcal{C}^* \subset \mathcal{P}_2(n)$ adding to $\mathcal{C}_0$ a "large" subcode of $\widehat{\mathcal{C}}_1$ in such a way that the distance $d_S(U,V)$ between all pairs (U,V) where $U \in \mathcal{C}_0$ and $V \in \mathcal{C}_1$ is at least three. Let us denote $p(n,q) = \sum_{k=1}^{n} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q /(q^k - 1)$. Note that this is a trivial upper bound for $D_q(n,1)$ (in view of bound II.6, applied for codes with minimum distance $d_S = 4$). Our code $\mathcal{C}^* \subset \mathcal{P}_2(n)$ has size $|\mathcal{C}^*| > 0,14p(n,2)$. Thus we have the following.

Theorem 8: $B_2(n,1) > 0,14p(n,2)$.

Construction

For our construction we need two simple observations. First we define matrices with $(0,1,*)$–entries. Let us denote by S_m^k the $k \times m$ matrix with a $*$ in each entry and by R_m^k the $k \times m$ matrix $[r_{i,j}]$ with entries $r_{k-1,m} = r_{k,m-1} = r_{k,m} = 0$ and $r_{i,j} = *$ elswhere.
Given integer $n \geq 2$ we define the matrices
$P_{n-2i} = [S_{n-2i}^{i-1}|I_{n-2i}|S_{n-2i}^{i+1}]$ for $1 \leq i \leq \lfloor \frac{n-2}{2} \rfloor$ and $P_{n-2i-1} = [R_{n-2i-1}^{i+1}|I_{n-2i-1}|S_{n-2i-1}^{i-1}]$ for $1 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$. We also define $P_n = I_n$, $P_0 = [0^n]$ and $P_1 = P_{n-1} = \emptyset$.
For each matrix P_{n-2i}, called a support matrix, we define the lifted code $(n, 4, n-2i)_q$-code, denoted by $\widehat{\mathcal{C}}_{n-2i}$, determined by the set of all matrices $[A_1|I_{n-2i}|A_2]$ where each $(n-2i) \times 2i$ matrix $[A_1|A_2]$ is a codeword of a given MRD code $\mathcal{C}_{n-2i} \subset \mathbb{F}_q^{(n-2i)\times 2i}$ with minimum distance $d_R = 2$. Similarly, for each matrix P_{n-2i-1} we define an $(n, 4, n-2i-1)_q$-code $\widehat{\mathcal{C}}_{n-2i-1}$ (which is a subcode of a lifted code) as follows. As before, we define a lifted code $\widehat{\mathcal{C}'}_{n-2i-1}$ determined by the matrices $[B_1|I_{n-2i-1}|B_2]$ where each $[B_1|B_2]$ is a codeword of a given MRD code $\mathcal{C}'_{n-2i-1} \subset \mathbb{F}_q^{(n-2i-1)\times(2i-1)}$ with minimum distance $d_R = 2$. But now we take the subcode $\mathcal{C}_{n-2i-1} \subset \mathcal{C}'_{n-2i-1}$ consisting of those matrices $[B_1|B_2]$ in which the $(n-2i-1)\times(i+1)$ matrices B_1 have zeros in the entries corresponding to the zeros of R_{n-2i-1}^{i+1} in P_{n-2i-1}. Correspondingly we get the subcode $\widehat{\mathcal{C}}_{n-2i-1}$, determined by $\mathcal{C}_{n-2i-1}$, of the lifted code $\widehat{\mathcal{C}'}_{n-2i-1}$. Note that $\widehat{\mathcal{C}}_n$ and $\widehat{\mathcal{C}}_0$ are trivial codes consisting of one element and $\widehat{\mathcal{C}}_1 = \widehat{\mathcal{C}}_{n-1} = \emptyset$.
It is easy to show that $|\widehat{\mathcal{C}}_{n-2i-1}| \geq |\widehat{\mathcal{C}'}_{n-2i-1}|/q^3$ for $1 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$. In fact, one has a more general statement (which directly follows from Lemma 1 or from Corollary 1 applied for space $\mathbb{F}_q^{n\times m}$).

Lemma 2: Given integers $n, m \geq 1$, let $J \subset \{1, \ldots, n\} \times \{1, \ldots, m\}$ and let $\mathcal{F}_J \subset \mathbb{F}_q^{n \times m}$ be a subset of all matrices which have fixed elements in all entries $(i, j) \in J$. Then for any rank-metric code $\mathcal{C} \subset \mathbb{F}_q^{n \times m}$ of minimum distance d_R there exists a code $\mathcal{C}(\mathcal{F}_J) \subset \mathcal{F}_J$ of the same minimum distance with $|\mathcal{C}(\mathcal{F}_J)| \geq |\mathcal{C}|/q^{|J|}$.

Since $|\widehat{\mathcal{C}}'_{n-2i-1}| \geq \frac{1}{4} A_q(n, 4, n-2i-1)$, we have $|\mathcal{C}_{n-2i-1}| \geq \frac{1}{4q^3} A_q(n, 4, n-2i-1)$.
We define now the code $\mathcal{C}^* = \bigcup_{j=0}^{n} \widehat{\mathcal{C}}_j$. Easy calculation shows that for $q = 2$ we have $|\mathcal{C}^*| > 0,14p(n, 2)$. It remains to show that the distance d_S between elements of two classes $\widehat{\mathcal{C}}_i$ and $\widehat{\mathcal{C}}_{i-1}$ is at least three.

Lemma 3: Given a field $\mathbb{F}$ and a matrix P_j (defined above), let $P_j(\mathbb{F})$ be a matrix obtained from P_j, such that its each entry with $*$ is replaced by an element of $\mathbb{F}$. Let also $\langle P_j(\mathbb{F}) \rangle$ be the rowspace of $P_j(\mathbb{F})$. Then for $3 \leq j \leq n-2$ and for all $\langle P_j(\mathbb{F}) \rangle$ and $\langle P_{j-1}(\mathbb{F}) \rangle$ we have

$$d_S(\langle P_j(\mathbb{F}) \rangle, \langle P_{j-1}(\mathbb{F}) \rangle) \geq 3. \qquad \text{(IV.1)}$$

Proof: Note that condition (IV.1) is satisfied iff $\langle P_j(\mathbb{F}) \rangle \not\supseteq \langle P_{j-1}(\mathbb{F}) \rangle$ for all $\langle P_j \rangle$ and $\langle P_{j-1} \rangle$ defined above. The latter can be easily shown observing that any matrix $\langle P_{n-2i} \rangle$ does not contain the last row of a matrix $P_{n-2i-1}(\mathbb{F})$ and any $\langle P_{n-2i+1}(\mathbb{F}) \rangle$ does not contain the first row of a matrix $P_{n-2i}(\mathbb{F})$. This fact is easy to realize on the example below. ■

Example: $n = 8$.

$P_8 = [I_8], \;\; P_0 = [0^8]$

$$P_6 = \begin{bmatrix} 1 & & & & & & * & * \\ & 1 & & & & & * & * \\ & & 1 & & & & * & * \\ & & & 1 & & & * & * \\ & & & & 1 & & * & * \\ & & & & & 1 & * & * \end{bmatrix}$$

$$P_5 = \begin{bmatrix} * & * & 1 & & & & & * \\ * & * & & 1 & & & & * \\ * & * & & & 1 & & & * \\ * & 0 & & & & 1 & & * \\ 0 & 0 & & & & & 1 & * \end{bmatrix}$$

$$P_4 = \begin{bmatrix} * & 1 & & & & * & * & * \\ * & & 1 & & & * & * & * \\ * & & & 1 & & * & * & * \\ * & & & & 1 & * & * & * \end{bmatrix}$$

$$P_3 = \begin{bmatrix} * & * & * & 1 & & & * & * \\ * & * & 0 & & 1 & & * & * \\ * & 0 & 0 & & & 1 & * & * \end{bmatrix}$$

$$P_2 = \begin{bmatrix} * & * & 1 & & * & * & * & * \\ * & * & & 1 & * & * & * & * \end{bmatrix}$$

Acknowledgement

The work of the second author is supported by DFG project AH46/8-1 "Information Flows in Networks".

References

[1] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, On perfect codes and related concepts, Des. Codes Cryptogr., vol. 22, no. 3, 221–237, 2001.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, Network information flow, IEEE Info. Theory, vol. 46, no. 4, pp. 1024-1016, 2000.

[3] A.E. Brouwer, A.M. Cohen, and A. Neumaier, *Distance regular graphs*, Springer-Verlag, Berlin Heidelberg, 1989.

[4] N. Cai and R. W. Yeung, Network error correction, Part II: Lower bounds, Communications in Information and Systems, vol. 6, no. 1, 37-54, 2006.

[5] Chou, Wu, and Jain, Practical network coding, in Proc. 2003 Allerton Conf. on Commun., Control and Computing, (Monticello, IL), Oct. 2003.

[6] Ph. Delsarte, An algebraic approach to associated schemes of coding theory, Philips J. Res., vol. 10, 1-97, 1973.

[7] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagram, CoRR, vol. abs/0807.4846, Oct. 2008.

[8] T. Etzion and A. Vardy, Error-correcting codes in projective spaces, in Proc. IEEE Int. Symp. Info. Theory, Toronto, July 2008, pp. 871-875.

[9] P. Frankl and R. Wilson, The Erdös-Ko-Rado theorem for vector spaces, J. Combin. Theory A, vol. 43, 228-236, 1986.

[10] E.M. Gabidulin, Theory of codes with maximum rank distance, Problems Info. Transmission, vol. 21, no. 1, 1-12, 1985.

[11] T. Ho, R. Kötter, M. Medard, D.R. Karger, and M. Effros, The benefits of coding over routing in randomized setting, Proc. 2003 IEEE Int. Symp. on Inform. Theory, (Yokohama) p. 442, June 20-July 3, 2003.

[12] T.Ho, M. Medard, R. Kötter, D.R. Karger, M. Effros, J. Shi, and B. Leong, A Random Linear Network Coding Approach to Multicast, IEEE Trans. on Info. Theory, vol. 52, no. 10, 4413-4430, 2006.

[13] D.J. Kleitman, On an extremal property of antichains in partial orders. The LYM property and some of its implications and applications. Combinatorics, Part 2: Graph theory; foundations, partitions and combinatorial geometry, pp. 77–90. Math. Centre Tracts, No. 56, Math. Centrum, Amsterdam, 1974.

[14] R. Koetter and F.R. Kschischang, Coding for Errors and Erasures in Random Network Coding, IEEE Trans. Info. Theory, vol. 54, no. 8, 3579 - 3591, 2008.

[15] S.-Y. R. Li, R. W. Yeung, and N. Cai, Linear network coding, IEEE Trans. Info. Theory, vol. 49, no. 2, 371-381, 2003.

[16] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1988.

[17] M. Schwartz and T. Etzion, Codes and anticodes in the Grassman graph, J. Combin. Theory Ser. A 97, no. 1, 27–42, 2002.

[18] D. Silva, F.R. Kschischang, and R. Koetter, A Rank-Metric Approach to Error Control in Random Network Coding, IEEE Trans. Info. Theory, vol. 54, no. 9, 3951 - 3967, 2008.

[19] H. Wang, C. Xing, and R. Safavi-Naimi, Linear authentification codes: bounds and constructions, IEEE Trans. Info. Theory, vol. 49, 866-872, 2003.

[20] S-T. Xia and F-W. Fu , Johnson type bounds on constant dimension codes, Des. Codes Cryptogr., vol. 50,163-172, 2009.

[21] R. W. Yeung and N. Cai, Network error correction, Part I: Basic concepts and upper bounds, Communications in Information and Systems, vol. 6, no. 1, 19-36, 2006.

[22] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, Network Coding Theory, now Publishers, 2005.