# Subspaces, Matrices and Codes

Eimear Byrne

## I. Introduction

The landscape of algebraic coding theory has undergone major changes in the last fifteen years. Network coding in particular has had a major impact on associated areas of discrete mathematics, giving rise to new research topics and reviving old ones.

This has been particularly apparent in the field of network error correction, after the seminal papers of [43], [61]. In the first of these, the authors offered a solution to multicast communication across noisy networks, using *random network coding*. In this model, at an intermediate node, random linear combinations of the incoming packets are output before continuing through the network. A set of some $n$ transmitted packets can then only be distinguished from another up to taking linear combinations. For this reason, they proposed using *subspace codes*, which are codes whose codewords are row spaces of sets of matrices with $n$ rows. In order to facilitate error correction, a distance function was identified, namely the subspace metric.

Aside from the practical applications to network communications, other aspects of the theory of subspace codes were met with great enthusiasm. Researchers with expertise in classical coding theory immediately set about tackling the question of optimality of subspace codes, finding upper bounds on the size and constructions of good codes [13], [25], [28], [29], [37], [40], [59], [63]. Work on code optimality led to a significant revival of interest in $q$-analogues of various combinatorial objects such as designs over finite fields. Since the original papers of Thomas [64], [65], there had been little written on the subject until very recently [6], [10], [11], [32], [41], [44], [46].

Central to the topic of subspace codes is that of *rank metric codes*, which are matrix codes, equipped with the *rank distance* function. Rank-metric codes provide constructions of some of the best subspace codes. Optimal matrix codes [18], [33] have been known for some decades. Delsarte-Gabidulin codes (also known as Gabidulin or generalized Gabidulin codes) became a subject of intense study especially after the connection to network error correction was made. They had already been considered for coding-based crytographic schemes [12] and there are many papers on decoding algorithms for such codes [7], [14], [33], [38], [47], [71]. This made them ideal for constructions of subspace codes, since in addition to yielding near-optimal codes, they brought with them ready-made decoding. Since then there have been numerous papers on the subject and more generally on the topic of *maximum rank distance* (MRD) codes, which are the rank-metric analogue of MDS codes.

As MRD codes exist in the form of Delsarte-Gabidulin codes for all parameters without restriction on the field size, it has only been very recently that any efforts were made to obtain infinite families outside of the class of Delsarte-Gabidulin codes [57]. The structure of MRD codes has generated a lot of interest as a topic in its own right [19], [20], [42], [51], [54], [56].

The relevance of rank-metric codes to network coding problems has not been confined to error correction in random network coding. They also arise in applications of linear coding to problems of *broadcast with side-information*. This is implicit in the literature for broadcast problems with coded-side information, although not commonly remarked upon explicitly. Such problems include index coding and coded-caching. The importance of index coding in network coding was established in [26], [31], where equivalences between the two problems were shown. Coded-caching in particular is currently a very active area of research after the work [52]. These broadcast problems involve efficient delivery of big data files to many users, each of whom already has some data stored locally in its cache via some form of placement, either

School of Mathematics and Statistics, University College Dublin, Ireland. e-mail: ebyrne@ucd.ie

randomly or by design. There is an extensive literature on the subject: [2], [3], [4], [5], [8], [9], [15], [52], [22], [23], [58], [68], [70]. In the case of linear coding, the structure of the cached data or side information can be expressed as a rank-metric code. The fundamental limits of transmission in these problems then relate to covering properties of matrix codes of this type.

In this letter we will give a brief survey of recent results on subspace codes and rank-metric codes which have evolved since random network coding for error correction became known to the community working in algebraic coding theory. Furthermore, we will make an explicit connection of rank-metric codes to broadcast with side-information problems. We will outline some achievements and identify open problems.

Throughout, we will let $\mathbb{F}_q$ denote a finite field of $q$ elements, for some prime power $q$. We write $\mathbb{F}_q^{n\times m}$ to denote the set of $n \times m$ matrices with entries in $\mathbb{F}_q$. In most of what follows we will assume that all matrices and vectors have coefficients in $\mathbb{F}_q$.

## II. Subspace and Matrix Codes

A matrix code $\mathcal{C}$ is a set of $n \times m$ matrices with entries in $\mathbb{F}_q$ and is referred to as a rank-metric code when associated with the rank distance function:

$$d_{\rm rk}(X, Y) = {\rm rk}(X - Y).$$

Without loss of generality we assume that $m \geq n$. If $\mathcal{C} \subset \mathbb{F}_q^{n\times m}$ is $\mathbb{F}_q$-linear of dimension $k$ and minimum distance $d$ we say it has parameters $[n \times m, k, d]_q$. In [18], (analogous to the Singleton bound) Delsarte showed that if $\mathcal{C}$ has minimum rank distance $d$ then

$$|\mathcal{C}| \leq q^{m(n-d+1)}.$$

Codes that meet Delsarte's bound are called *maximum rank distance* (MRD) codes.

Rank metric codes have been considered for several applications in communications theory and cryptography. An explicit construction for MRD codes was given independently in [18] and [33]. Several authors have worked extensively on decoding algorithms for this class of Delsarte-Gabidulin codes [7], [14], [38], [47], [71].

We briefly explain the connection to subspace codes for random network coding with error correction. One noisy channel model for matrix codes is represented by

$$X \longrightarrow Y = AX + BZ,$$

where the matrix $X$ is transmitted and the matrix $Y$ is received. This can be associated with a network, where $Z$ is an error matrix and $A$ and $B$ are the *transfer matrices* [45], which are unknown, so no knowledge of the network topology is assumed (which is the point of random coding). In the error-free case, $A$ is invertible and $Z$ is zero. Then $AX$ is received, from which a user cannot deduce $X$ but can identify its row space, $\langle X\rangle$. For this reason each message is encoded to a unique subspace, which can be identified with a unique reduced-row echelon form matrix.

A subspace code is a set subspaces of $\mathbb{F}_q^m$. If all its codewords have the same dimension $k$ (as we'll assume here), it is called a *constant dimension* subspace code (CDC). It is usually equipped with the subspace distance:

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

Given a pair of matrices $X, Y$, we can form a new pair of matrices in canonical form, $[I, X], [I, Y]$ and we get

$$d_S(\langle [I, X]\rangle, \langle [I, Y]\rangle) = 2d_{\rm rk}(X - Y).$$

Then a rank-metric code in $\mathbb{F}_q^{n\times m}$ yields a CDC of constant dimension $n$. This is the *lifting* construction used in [61] which gives a practical scheme for decoding subspace codes using a rank-metric decoder, in

particular, one for the Delsarte-Gabidulin codes. Asymptotically, the resulting codes are optimal, but for smaller parameters are not.

We remark at this point that there is a simple, low-complexity encoding/decoding scheme for matrix channels given in [60] that corrects error matrices of some fixed rank $t$, under the assumption that a basis of the error matrix occurs in the first $v$ rows. The authors refer to this as *error trapping*. The probability of a decoding error under this scheme is at most

$$2t(q^{1+v-t})^{-1}.$$

### A. The Main Subspace Coding Problem

This still leaves open the general question of optimality of subspace codes, the Main Subspace Coding problem. Many variants on lifting constructions have been explored using ideas from combinatorics and geometry [28], [27], [63] and many bounds on the size of an optimal subspace code have been derived (see [25], [37], [40] and the references therein). Many of these constructions have the simple lifted MRDs of [61] as subcodes. A highly useful resource for interested researchers is given by [40], where the authors have written a collection of the known upper bounds on the size of an optimal subspace code, which includes links to parameter tables and an extensive list of the literature.

The *multilevel construction* of [28] was very successful in producing good CDCs. Their approach uses constant weight Hamming codes and Ferrers diagrams [69, Chapter 16]. A Ferrers diagram arises in combinatorics as a means of representing partitions of an integer. For example, the sum $4+2+2$ is represented as a $3 \times 3$ array of dots and blanks, with 4 dots in the first row and 2 dots in the 2nd and 3rd rows. The dots of the array are arranged to have an echelon type form. Then a rank-metric *Ferrers diagram code* is constructed and lifted to yield a subspace code. An $[n, m, \delta]$ Ferrers diagram rank-metric code is formed by completions of an $n \times m$ matrix associated with a given Ferrers diagram $\mathcal{F}$, with zeroes appearing outside of the coordinates corresponding to the dots of $\mathcal{F}$ in such a way that the resulting code has minimum rank distance $\delta$. Theorem 1 of [28] gives an upper bound on the dimension of such a code as the minimum number of dots that do not appear in the first $i$ rows and the rightmost $\delta - 1 - i$ rows over all $i \in \{0, .., \delta - 1\}$.

**Example II.1.** Let $x = [1001100]$. To construct a 3-dimensional space over $\mathbb{F}_q$, identify $x$ with its unique echelon-Ferrers form matrix:

$$\begin{bmatrix} 1 & \bullet & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{bmatrix} \qquad \begin{matrix} \bullet & \bullet & \bullet & \bullet \\ & & \bullet & \bullet \\ & & \bullet & \bullet \end{matrix}$$

The Ferrers diagram on the right is used to produce a rank-metric Ferrers diagram code, whose dimension is at most 2 for $\delta = 2$, according to the bound of [28]. This rank-metric code is lifted to a CDC of constant dimension 3 by embedding its matrices into the echelon-Ferrers matrix of $x$ and taking all row spaces as subspaces. If we repeat this procedure with other binary vectors that form a constant Hamming weight code and take the union of the resulting subspace codes, we arrive at a larger CDC.

These ideas were further developed in [63], additionally using matchings of the complete graph to obtain some of the best known CDS for the *injection distance*.

**Open Problem II.2.** *In [27], the authors give a number of constructions of optimal Ferrers diagam rank metric codes, which are optimal or near-optimal with respect to the Ferrers diagram bound [28, Theorem 1]. Such codes can be lifted to give good subspace codes. However, it is not known if the bound cannot be attained in some cases. The authors suggest that this question could be answered by finding large non-linear rank-metric* anticodes*, which are codes whose words have ranks upper-bounded by a given number. Anticodes for the rank metric are studied in much more detail in [34].*

An intriguing example of an optimal subspace code relates to a $q$-analogue of design theory. Let $\mathcal{C}$ be a CDC of constant rank $k$ in $\mathbb{F}_q^n$ such that every $t$-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one member of $\mathcal{C}$. Then $\mathcal{C}$ is called an $S_q(t,k,n)$ Steiner structure (or a $q$-Steiner system), which is also an optimal subspace code. A *spread*, which is a splitting of a vector space into subspaces with trivial intersection, is an example of an $S_q(1,k,ks)$. A tantalizing first question is on the existence of a $q$-analogue of the *Fano Plane*, which for $q=2$ would be an $S_2(2,3,7)$ having 381 3-dimensional spaces (planes) as codewords (from a choice of 11811 in $\mathbb{F}_2^7$) with every pair of lines (2-dimensional spaces) contained in a unique plane. It is still unknown if this 2-design over $\mathbb{F}_2$ exists.

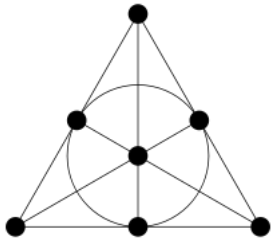

Fig. 1. A graphical representation of the classical Fano plane, with 7 points and 7 lines. Every pair of points is contained in a unique line.

It was a few years before the existence question of a non-trivial $S_q(t,k,n)$ was rewarded with an actual example. It was finally shown in [6] there exists an $S_2(2,3,13)$ (in fact at least 401 non-isomorphic ones). This sporadic example was discovered by computer search, applying the Kramer-Mesner method under the assumption of it having a large group of symmetries, making the computation feasible. To give an idea of the scale of such a problem, this parameter set produces a code with 1,597,245 3-dimensional spaces as codewords. Searching for the next cases using this method is not tractable at this time. No other non-trivial examples are known. If the $q$-Fano plane does exist, its symmetry group would be very small, possibly trivial [44] making a search by computer infeasible (for now). An interesting connection to the existence of *skew affine* $q$-Steiner systems was given in [72].

**Open Problem II.3.** *Does there exist an $S_2(2,3,7)$? A computer-free construction of a CDC of constant dimension 3 and minimum subspace distance 4 in $\mathbb{F}_2^7$ with largest known number of codewords (329) is given in [41], as an example of a general method for dimension 3 CDCs. The authors use expurgation and augmentation to modify a lifted Delsarte-Gabidulin code with the aim of obtaining an optimal code or indeed the $q$-Fano plane. If the $S_2(2,3,7)$ does exists, it may be possible to obtain it by modifying this approach, using a different class of MRD codes.*

**Open Problem II.4.** *Does the $S_2(2,3,13)$ example occur as part of an infinite family of $q$-Steiner systems? Do other examples exist? Are there algebraic constructions for $q$-Steiner systems?*

### *B. MRD Codes*

There are a few equivalent representations of the Delsarte-Gabidulin MRD codes. An elegant construction uses *linearized polynomials* (see [50], [55] for properties of such polynomials). A linearized polynomial in $\mathbb{F}_{q^n}[x]$ is one of the form:

$$f = f_0 x + f_1 x^q + \cdots f_{k-1} x^{q^{k-1}},$$

with $f_i \in \mathbb{F}_{q^n}$. Then $f$ represents an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$ and so can be identified with an $n \times n$ matrix with coefficients in $\mathbb{F}_q$, after choosing some basis of $\mathbb{F}_{q^n}$ for the scalar field $\mathbb{F}_q$. We refer the reader to [57] to see an explicit worked example of this correspondence, which we omit here due to space constraints. Matrix multiplication corresponds to composition of functions modulo $x^{q^n} - x$ and the rank of $f$ is at

least $n-k+1$, as the dimension of its kernel is at most $k-1$. The polynomial representation can offer useful insights to the structure of rank-metric codes.

The most general infinite family of MRD codes known to date was presented by Sheekey in [57]. For brevity we'll give this for $m=n$, so for $[n\times n, nk, n-k+1]_q$ codes. Such a code has the form: $\mathcal{H}_k(\nu,h) :=$

$$\{f_0x + f_1x^q + \cdots + f_{k-1}x^{q^{k-1}} + \nu f_0{}^{q^h}x^{q^k} : \nu, f_i \in \mathbb{F}_{q^n}\},$$

where $\nu^{\frac{q^n-1}{q-1}} \neq (-1)^{nk}$. This includes the family of Delsarte-Gabidulin codes, which are precisely those for which $\nu = 0$. Note that the Delsarte-Gabidulin codes in $\mathbb{F}_q^{n\times n}$ are $\mathbb{F}_{q^n}$-linear, whereas for $\nu \neq 0$, $\mathcal{H}_k(\nu,h)$ may not be, depending on the value of $h$.

In [42], the authors give a simple criterion for checking if an MRD code is a Delsarte-Gabidulin code and use this to produce sporadic examples of MRD codes that do not fall into this category. In fact 'most' MRD codes are not Delsarte-Gabidulin codes; that is, the property of being MRD and non-Delsarte-Gabidulin are *generic* [53]. It is likely, although not yet proven in the literature, that the codes $\mathcal{H}_k(\nu,h)$ also do not encompass 'most' MRD codes.

The rank *weight distribution*, (the number of codewords of each possible weight) of an MRD code is determined by its parameters $[n\times m, m(n-d+1), d]_q$ [18]. The dual code of an $\mathbb{F}_q$-linear matrix code $\mathcal{C}\subset\mathbb{F}_q^{n\times m}$ is given by

$$\mathcal{C}^\perp := \{Y \in \mathbb{F}_q^{m\times n} : \mathrm{Tr}(\mathrm{XY}^{\mathrm{T}}) = 0 \ \forall\ \mathrm{X}\in\mathcal{C}\},$$

where $\mathrm{Tr}(A)$ is the usual trace of a square matrix $A$, the sum of its diagonal elements. This definition follows from the fact that $\langle X, Y\rangle := \mathrm{Tr}(\mathrm{XY}^{\mathrm{T}})$ is an inner product on $\mathbb{F}_q^{n\times m}$. As is usual in algebraic coding theory, study of the dual code plays an important role. $\mathcal{C}$ is a linear MRD code if and only if its dual is MRD, equivalently, if and only if

$$d + d^\perp = n + 2.$$

There has been much recent activity on the structure of MRD codes [19], [20], [35], [54], [51]. Unlike MDS codes, their classical analogues, MRD codes exist for all choices of $q, m, n, d$. Mac Williams' duality theorem holds for rank-metric codes [18], [36], [56] (although Mac Williams' extension theorem does not).

Gadouleau and Yan are among the few authors who have considered covering properties of rank-metric codes [35]. The covering radius of a rank-metric code $\mathcal{C}\subset\mathbb{F}_q^{n\times m}$ is defined as

$$\begin{aligned}\rho(\mathcal{C}) &:= \max\{\min\{d_{\mathrm{rk}}(R,C) : C\in\mathcal{C}\} : R\in\mathbb{F}_q^{n\times m}\}\\ &:= \max\{d_{\mathrm{rk}}(R,\mathcal{C}) : R\in\mathbb{F}_q^{n\times m}\}.\end{aligned}$$

The covering radius of a code is a fundamental parameter that reflects the maximum weight of any error correctable by that code. The general covering problem is to determine the least number of spheres of a given radius that cover the underlying space. The most interesting codes in this respect are those with low covering radius. It has been extensively studied in the Hamming metric, where it has played a role in different applications, such as data compression. In general, determining the covering radius of a code is hard, as are constructing families with specified covering radius.

There are however, some bounds on the covering radius for the Hamming case [16] that follow without much difficulty to the rank-metric case. The author has shown, for example, following the arguments of [17], that the covering radius of a rank-metric code is upper bounded by the number of weights of its dual code (or in the non-linear case by its *external distance*).

**Example II.5.** Let $n=rs$ and let $\mathcal{C}$ be the $[n\times n, nr, s]_q$ code

$$\mathcal{C} = \left\{\sum_{i=0}^{r-1} f_i x^{q^{si}} : f_i\in\mathbb{F}_{q^n}\right\}.$$

Then $\mathcal{C}$ has $r$ non-zero rank weights $\{s, 2s, ..., rs\}$ over $\mathbb{F}_q$, so that $\rho(\mathcal{C}^\perp) \leq r$.

We mention a few fundamental upper and lower bounds on the covering radius that are independent of the metric used.

- The *sphere-covering bound* gives a lower bound on the covering radius of a code:
$$\rho(\mathcal{C}) \geq \{N : V_q(n, m, N)|\mathcal{C}| \geq q^{nm}\},$$
where $V_q(n, m, N) = \{A \in \mathbb{F}_q^{n\times m} : \mathrm{rk}(A) \leq N\}$ is the volume of a sphere of radius $N$ about a matrix in $\mathbb{F}_q^{n\times m}$.
- If $\mathcal{C} \subset \mathcal{C}' \subset \mathbb{F}_q^{n\times m}$ then the covering radius of $\mathcal{C}$ is lower-bounded by the minimum distance of $\mathcal{C}'$:
$$\rho(\mathcal{C}) \geq d_{\mathrm{rk}}(\mathcal{C}').$$
- If $\mathcal{C}$ is *maximal*, i.e. is not a proper subset of another code for the same minimum distance $d$, then
$$\rho(\mathcal{C}) \leq d - 1.$$

Many other upper and lower bounds appear in [35].

While the weight distribution of an MRD code in $\mathbb{F}_q^{n\times m}$ is determined by its minimum distance, its covering radius is not. Any MRD code $\mathcal{C}$ is clearly maximal, being optimal. In the case of the MRD codes $\mathcal{H}_k(\nu, h)$, the covering radius attains this last bound with equality; that is, it is an $[n \times n, n(n-d+1), d]_q$ rank metric code with covering radius $d-1$. This can be seen by observing that these form a nested class of MRD codes. However, there are examples of MRD codes outside this class with covering radius less than $d - 1$.

**Open Problem II.6.** *Can the construction of [57] be extended, or is this the largest infinite family of MRD codes that contains the Delsarte-Gabidulin codes? Do there exist other infinite families of MRD codes?*

**Open Problem II.7.** *Can the criterion for Delsarte-Gabidulin codes of [42], or a variant of it, be extended to include the larger class of MRD codes [57]? If so then the probability of an arbitrary MRD code being in this family of codes could be upper-bounded.*

**Open Problem II.8.** *Find other infinite families of rank-metric codes with covering radius $d - 1$.*

## III. Broadcast with Side-Information

Rank-metric codes also appear in broadcast problems. Consider the following broadcast with side information scenario. The data vector $x$ below may have coefficients in a field $\mathbb{F}_{q^t}$, but we assume that all other matrices and vectors have coefficients in $\mathbb{F}_q$.

- There is a single sender and $m$ receivers.
- $x = [x_1, ..., x_n]$ is the uncoded data held by the sender.
- User $i$ has side information $(V_i, xV_i)$, for some $n \times v_i$ matrix $V_i = [V_i^1, ..., V_i^{v_i}]$ of rank $v_i$ .
- User $i$ has request matrix $R_i = [R_i^1, ..., R_i^{r_i}]$, an $n \times r_i$ matrix of rank $r_i$.
- User $i$ demands request packet $xR_i$.
- The sender, after receiving each request $R_i$, broadcasts
$$Y = xL$$
for some $n \times N$ matrix $L$, $N < n$.
- Each user decodes $xR_i$ by solving a linear system of equations in the received $Y$ and its side-information.

The sender is faced with the following broadcast problem: find an encoding matrix $L$ that minimizes $N$ such that the demands of all users satisfied.

We say that $L$ realizes a length $N$ code for this problem if indeed each user can retrieve its demand $xR_i$ for any source data vector $x$, given knowledge of

$$L, xL, V_i, xV_i.$$

The source data $x$ should be thought of as a variable in the above *instance* of the broadcast with side-information problem. If such an $L$ exists, we say that the length $N$ is achievable for the given instance. It is a computationally hard problem, NP-hard in fact, to find such $L$ realizing a minimal length encoding.

User $i$ can retrieve its demand $xR_i$, for all possible choices of $x$ if and only if there exist matrices $A_i, B_i$ satisfying

$$R_i = V_iA_i + LB_i,$$

from which it decodes $xR_i$, knowing $xV_i$ (as its side information) and $xL$ (which was transmitted). It is generally assumed that a user does not demand $xR_i$ if it already has it in its cache. Therefore, we assume that no column of $R_i = [R_i^1, ..., R_i^{r_i}]$ is contained in the column space of $V_i$, so in other words $R_i^j \neq V_ia$ for any vector $a$.

We now describe this in terms of a matrix code. First let $r = \sum_{j=1}^m r_j$ and let $R$ be the $n \times r$ matrix

$$R = [R_1, R_2, ..., R_m].$$

We call $R$ the request matrix. For each $i$, let

$$\mathcal{C}_i = \{V_iA : A \in \mathbb{F}_q^{v_i \times r_i}\} \subset \mathbb{F}_q^{n \times r_i}.$$

So $\mathcal{C}_i$ is a vector space of $n \times r_i$ matrices for the scalars $\mathbb{F}_q$. It can be thought of as $r_i$ copies of the length $n$ linear code generated by the columns of $V_i$. Now define

$$\mathcal{C} = \{[U_1, U_2, ..., U_m] : U_i \in \mathcal{C}_i\} \subset \mathbb{F}_q^{n \times r},$$

which is a vector space of $n \times r$ matrices for the scalars $\mathbb{F}_q$. We call this matrix code $\mathcal{C}$ the side-information code.

We say that the pair $(R, \mathcal{C})$ is an instance of the broadcast with side-information problem. The problem of determining the optimal code length of the instance $(R, \mathcal{C})$ and a corresponding encoding matrix $L$ is a *delivery* problem.

It can easily be shown that the minimum length of a code for $(R, \mathcal{C})$ is

$$\kappa(R, \mathcal{C}) := \min\{\mathrm{rk}(R + C) : C \in \mathcal{C}\}.$$

The set $R + \mathcal{C} := \{R + C : C \in \mathcal{C}\}$ is a coset or translate of $\mathcal{C}$, so $\kappa(R + \mathcal{C})$ is the minimum rank of any member of this coset. It is also the rank distance of the matrix $R$ to the side information code $\mathcal{C}$. This generalizes the *minrank* of a *side-information graph* or hypergraph, as it arises in the *index coding problem* (cf. [3], [4], [49], [23]). Implicit in this is the fact that any full-rank matrix $L$ that realizes the instance $(R, \mathcal{C})$ can be obtained by rank-factorization of a member of $R + \mathcal{C}$. Note that

$$\dim \mathcal{C} = \sum_{i \in [m]} r_iv_i$$

over $\mathbb{F}_q$, so $|R + \mathcal{C}| = q^s$ where $s = \sum_{i \in [m]} r_iv_i \leq rn$.

For a given side-information code $\mathcal{C}$, the sender can satisfy any set of requests in at most $\rho(\mathcal{C})$ transmissions, the rank-metric covering radius of the code $\mathcal{C}$. So if the side-information code $\mathcal{C}$ has low covering radius, then all instances of this broadcast problem require a small number of transmissions. Different variations and applications of the problem will however assume some restriction on the choice of possible request matrices $R$ that give a *valid* instance $(R, \mathcal{C})$. Then for given $\mathcal{C}$, the sender can satisfy any valid set of requests using at most

$$\begin{aligned} \rho_{\mathcal{R}}(\mathcal{C}) &:= \max\{\kappa(R, \mathcal{C}) : R \in \mathcal{R}(\mathcal{C})\} \\ &= \max\{d_{\mathrm{rk}}(R, \mathcal{C}) : R \in \mathcal{R}(\mathcal{C})\} \end{aligned}$$

transmissions, where $\mathcal{R}(\mathcal{C})$ denotes some set of valid request matrices in $\mathbb{F}_q^{n\times r}$.

This relates to a *placement* problem: that of determining side-information codes $\mathcal{C}$ with smallest covering radius or smallest restricted covering radius (where the radius is restricted to a subset $\mathcal{R}(\mathcal{C}) \subset \mathbb{F}_q^{n\times r}$).

As both quantities $\kappa(R,\mathcal{C})$ and $\rho_{\mathcal{R}}(\mathcal{C})$ are hard to compute, bounds and estimates are sought on them.

We remark that if $\mathcal{R}(\mathcal{C})$ is the set of request matrices $R$ such that no column of $R_i$ is contained in the column space of $V_i$ for any $i$, i.e. if

$$\mathcal{R}(\mathcal{C}) = \{R \in \mathbb{F}_q^{n\times r} : R_i^j \neq V_i a, \text{ any } a \in \mathbb{F}_q^{v_i}, i \in [m], j \in [r_i]\}$$

then

$$\rho_{\mathcal{R}}(\mathcal{C}) = \rho(\mathcal{C}).$$

Clearly, $\rho_{\mathcal{R}}(\mathcal{C}) \leq \rho(\mathcal{C})$. To see the converse, let $R \in \mathbb{F}_q^{n\times r}\backslash\mathcal{R}(\mathcal{C})$ satisfy $d_{\mathrm{rk}}(R,\mathcal{C}) = \rho(\mathcal{C})$. Without loss of generality, we may assume that $R$ has the form

$$R = [X_1, O|X_2, O|...|X_m, O],$$

for some matrices $X_i \in \mathbb{F}_q^{n\times c_i}$ such that no column of $X_i$ is contained in the column space of $V_i$ for any $i$ and where $O$ is the $n \times (r_i - c_i)$ zero matrix. Let $R' = [X_1, ..., X_m]$ and let $\mathcal{C}'$ be the matrix code found by deleting the coordinates of $\mathcal{C}$ in $[r]$ corresponding to the zero columns of $R$. Let

$$S = [X_1, Y_1|X_2, Y_2|...|X_m, Y_m] \in \mathcal{R}(\mathcal{C}),$$

for some matrices $Y_i$. Then

$$\rho(\mathcal{C}) = d_{\mathrm{rk}}(R,\mathcal{C}) = d_{\mathrm{rk}}(R',\mathcal{C}') \leq d_{\mathrm{rk}}(S,\mathcal{C}) \leq \rho(\mathcal{C}).$$

It follows that given any $R \in \mathbb{F}_q^{n\times r}\backslash\mathcal{R}(\mathcal{C})$ at distance $\rho(\mathcal{C})$ to $\mathcal{C}$, there exist some $S \in \mathcal{R}$ at distance $\rho(\mathcal{C})$ to $\mathcal{C}$. In particular, any lower bounds on $\rho(\mathcal{C})$ may be applied to $\rho_{\mathcal{R}}(\mathcal{C})$ for this set of valid request matrices.

**Open Problem III.1.** *Obtain further bounds on $\kappa(R,\mathcal{C})$ and $\rho(\mathcal{C})$ for codes $\mathcal{C}$ with the structure of a side-information code. There are several bounds on $\kappa(R,\mathcal{C})$ already known from the index coding with side information problem, but the best of these are inexplicit bounds [4], [5], [9], [58], [67].*

**Open Problem III.2.** *There has been limited activity so far on the subject of error correction in the broadcast with side information problem. Many of the known algorithms are based on syndrome decoding [4], [23]. Find lower complexity algorithms for error correction.*

**Open Problem III.3.** *Design side-information codes $\mathcal{C}$ with low rank metric covering radius, or infinite families of such codes.*

### *A. The Index Coding Problem*

The delivery problem for a fixed instance $(R,\mathcal{C})$ is a *scalar* linear index coding problem if $x$ has coefficients in $\mathbb{F}_q$ and is a *vector* linear index coding problem if $x$ has coefficients in $\mathbb{F}_{q^t}$ for $t > 1$. In the vector linear case, $x$ has components of block length $t$. The block length does not affect the minrank parameter, however, due to overhead transmission costs, the gains of index coding are greater as $t$ increases.

It is common in the index coding literature to assume that $R_i$ is a vector over $\mathbb{F}_q$ of length $n$, so that each user requests a single packet (so $r_i = 1$ for each $i$ and $r = m$). This is because in the event of a user requesting two packets, that user can be represented as two users with the same side-information and the problem essentially remains unchanged, from the index coding point of view.

In the original version of the index coding problem [2], [3], [8], [9], we have $m = n$, $R_i$ is a standard basis vector $e_i$ (so the $i$th component of $x$ is demanded by the $i$th user) and the matrices $V_i$ all have standard basis vectors as columns (so each user has components $x_j$ if the $j$th row of $V_i$ is non-zero). This

formulation identifies an instance with an underlying graph, or more generally, for $m \geq n$, a hypergraph [22], [23]. In [21] the authors introduce the problem for arbitrary request vectors $R_i$ and matrices $V_i$ using the term index coding with *coded side information*.

**Example III.4.** We describe an instance of the original index coding problem. Let $m = n = 7$ and $q = 2$. Let

$$V_1 = \begin{bmatrix} 0100000 \\ 0010000 \end{bmatrix}, V_2 = \begin{bmatrix} 0000010 \\ 0000001 \end{bmatrix}, V_3 = \begin{bmatrix} 0000100 \\ 0000001 \end{bmatrix}, V_4 = \begin{bmatrix} 0100000 \\ 0000100 \end{bmatrix},$$
$$V_5 = \begin{bmatrix} 1000000 \\ 0000010 \end{bmatrix}, V_6 = \begin{bmatrix} 0010000 \\ 0001000 \end{bmatrix} V_7 = \begin{bmatrix} 1000000 \\ 0001000 \end{bmatrix},$$

and $R_i = e_i$ ($i$th standard basis vector) for $i = 1, ..., 7$. So $R$ is the identity matrix and the $i$th user wants the $i$th bit of $x$. The coset $R + \mathcal{C}$ is a set of $2^{14} = 16384$ matrices of the form

$$\begin{bmatrix} 1 & \bullet & \bullet & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 1 & 0 & \bullet & 0 & \bullet \\ 0 & \bullet & 0 & 1 & \bullet & 0 & 0 \\ \bullet & 0 & 0 & 0 & 1 & \bullet & 0 \\ 0 & 0 & \bullet & \bullet & 0 & 1 & 0 \\ \bullet & 0 & 0 & \bullet & 0 & 0 & 1 \end{bmatrix}$$

where each dot $\bullet$ may be filled with $0$ or $1$. It can be checked that this coset has rank weight distibution

$$(4, 1), (5, 238), (6, 6575), (7, 9570).$$

In particular, it has exactly one matrix of minimal rank $4$, which is

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

In fact this is the incidence matrix of the Fano plane. (It is known that incidence matrices of structures like these have rank at most $(n + 1)/2$.) Let $\mathcal{R}(\mathcal{C}) = \{R \in \mathbb{F}_q^{7\times 7} : R_i \notin \mathcal{C}_i \text{ any } i \in [7]\}$. If we compute $\kappa(R, \mathcal{C})$ for $\mathcal{C}$ as above and for $R$ a permutation matrix in $\mathcal{R}(\mathcal{C})$, we find that it takes the value 3 for $1\%$ of instances, 4 for $62\%$ of instances and 5 for $37\%$ instances so the expected optimal number of transmissions if the request vectors are linearly independent is 4.35.

Feasible (not necessarily optimal) solutions to the index coding problem, i.e. determination of an encoding matrix $L$, can be found by various methods of partitioning an instance into simpler ones, for which an optimal solution is known. In the literature, these first appeared as graph-theoretic algorithms based on *clique covering*, *multicast partition* and their variants [9], [58], [67], but have been shown also to have analogues in the general case [5]. These use integer and linear programming to obtain coding partitions.

If we have $m \geq n$, each request matrix $R_i$ a standard basis vector and no restriction on the $V_i$, then determining $L$ of optimal or near-optimal length can be identified with a *low-rank matrix completion* problem. A greedy algorithm for the application to index coding was outlined in [49]. For wireless applications (so for matrices over the reals), the problem has been addressed in [39], [68]. While there are many algorithms for low-rank matrix completion problems over $\mathbb{R}$, few are known for matrices over finite fields. Even less is known for the most general case.

**Open Problem III.5.** *Find efficient algorithms for low-rank matrix completions arising in the index coding problem over finite fields.*

### B. The Coded-Caching Problem

The delivery phase of the *canonical coded-caching* problem [52] is the following specialisation of the instance $(R, \mathcal{C})$. First it is assumed that the $n$ packets of $x$ comprise $k$ blocks $x^1, ..., x^k$ of size $\ell$ (so that $n = k\ell$) and that each $i$th user wants some complete block, say $x^j$, after delivery. So $R_i$ is an $n \times r_i$ matrix

$$R_i = [O \cdots H^T \cdots O]^T$$

for some $\ell \times r_i$ matrix $H$ with standard basis vectors of length $\ell$ as columns. Each user has a subset of some number of packets from each block and the same number of packets $v$ in total. In terms of $(R, \mathcal{C})$, this imposes the constraints that for each $i$,

- $V_i$ is an $n \times v$ matrix,
- $R_i$ and $V_i$ have standard basis vectors as columns,
- the $j$th block of $\ell$ rows of $V_i$ has some $\ell - r_i$ standard basis vectors of length $\ell$ as columns that complete $H$ to a basis of $\mathbb{F}_q^\ell$.

For example, if user $i$ has the last $\ell - r_i$ packets of $x^j$ in its cache then $R_i$ and $V_i$ have the form,

$$R_i = \begin{bmatrix} O \\ \vdots \\ O \\ A|0 \\ O \\ \vdots \\ O \end{bmatrix} \quad V_i = \begin{bmatrix} * & O \\ * & \vdots \\ * & O \\ * & 0|B \\ * & O \\ * & \vdots \\ * & O \end{bmatrix},$$

where $[A|B]$ is an $\ell \times \ell$ permutation matrix. So valid choices of $\mathcal{C}$ and $R$ for consideration in the canonical coded caching problem are those satisfying the above. If a subset of users wish to receive the same block, the delivery to that set of users becomes a local multicast problem.

What distinguishes the coded-caching problem from the index coding problem is the role of the sender in the placement phase. If the index coding problem is essentially one of delivery for given $(R, \mathcal{C})$, central to the coded caching problem is optimal placement of the side-information code $\mathcal{C}$ in advance of knowing users' request matrix $R$. The sender seeks to choose $\mathcal{C}$ in such a way that the encoding matrix $L$ can deliver all requests $xR_i$ with a minimal number of transmissions. Thus the problem is to determine $\mathcal{C}$ such that $\rho_{\mathcal{R}}(\mathcal{C})$ is minimized, or to minimize this number for all valid choices of $\mathcal{C}$. In [52] the authors use the cut-set bound to derive a lower bound on the optimal storage memory rate trade-off. Furthermore, they devise a scheme that achieves this rate within a constant factor. So asymptotically, the canonical coded caching problem is solved. Moreover, it was shown in [70] that improvements to the scheme presented in [52] can only be achieved by considering caching schemes with coded side-information.

For example, the matrices $V_i$ may have columns that are not standard basis vectors, which corresponds to the cache data (the side-information) being encoded. Then $\mathcal{C}_i$ is an arbitrary $nv$-dimensional matrix code for each $i$. In [66] the authors propose a scheme for coded-caching with coded side-information using MDS and rank metric codes. Their scheme delivers an improvement in the memeory-rate trade-off of several known schemes and are in some cases optimal. However, their scheme requires large field sizes.

**Open Problem III.6.** *Modify current rank-metric sphere covering bounds to obtain lower bounds on the restricted covering radius for a side-information code $\mathcal{C}$.*

**Open Problem III.7.** *Obtain good caching schemes for smaller field sizes. Construct codes with low restricted covering radius for the coded caching problem.*

## IV. Concluding Remarks

Advances in finite geometry, combinatorics, algebraic coding theory and lattices have been made as a direct result of interest in network coding problems. It is the hope of the author that some small demonstration has been made of the great impact of this field on mathematics. It seems reasonable to expect that rank-metric codes will continue to play a dominant role in network communications theory and many more open problems remain to be solved.

Much of the research described here was conducted by participants in the EU COST Action *Random Network Coding and Designs over* $GF(q)$. A great deal more work than has been mentioned here was carried out as part of that action (see http://www.network-coding.eu/), including projects on distributed storage and cryptography and practical schemes for network coding.

## References


[1] N. Alon, A. Hassidim, E. Lubetzky, U. Stav, and A. Weinstein, "Broadcasting with Side Information", in Proc. 49th Annu. IEEE Symp. on Found. of Comput. Sci. (FOCS), pp. 823832, 2008.

[2] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", in Proc. 47th Annu. IEEE Symp. Found. Comput. Sci., 2006, pp. 197–206.

[3] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", IEEE Transactions on Information Theory, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[4] E. Byrne and M. Calderini, "Error Correction for Index Coding with Coded Side Information,", arXiv preprint, 1506.00785, 2015.

[5] E. Byrne and M. Calderini, "Bounding the Optimal Rate of the ICSI and ICCSI Problems,", arXiv preprint 1604.05991, 2016.

[6] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, A. Wassermann, "Existence of q-Analogs of Steiner Systems," Forum of Mathematics, Pi, to appear (see arXiv:1304.1462).

[7] M. Bossert, E. Gabidulin, "Codes for network coding," 2008 IEEE International Symposium on Information Theory, pp. 867–870

[8] Y. Birk and T. Kol, "Informed Source Coding on Demand (ISCOD) over Broadcast Channels", in Proc. IEEE Conf. Comput. Commun., San Francisco, CA, 1998, pp. 1257–1264.

[9] A. Blasiak, R. Kleinberg, E. Lubetsky, "Broadcasting With Side Information: Bounding and Approximating the Broadcast Rate," IEEE Transactions on Information Theory, vol. 59, no. 9, 2013, pp. 5811–5823.

[10] M. Braun, M. Kiermaier, Nakić, "On the Automorphism Group of a Binary $q$-Analog of the Fano Plane," Eur. J. Comb. 51, 2016.

[11] M. Braun, A. Kohnert, P. R. J. Östergard, A. Wassermann, "Large Sets of t-Designs over Finite Fields," Journal of Combinatorial Theory, Series A, Vol 124, pp.195202, 2014.

[12] T. Berger, P. Loidreau, "How to Mask the Structure of Codes for a Cryptographic Use," Designs, Codes and Cryptography, Volume 35, Issue 1, pp. 6379, 2005.

[13] C. Bachoc, A. Passuello, and F. Vallentin, "Bounds for Projective Codes from Semidefinite Programming," Advances in Mathematics of Communications 7, pp. 127-145, 2013.

[14] H. Bartz, V. Siderenko, "Algebraic Decoding of Folded Gabidulin Codes," Des. Codes Crypt., Online First, pp. 1–16 March 2016.

[15] Z. Chen, "Fundamental limits of caching: Improved bounds for small buffer users," arXiv preprint arXiv:1407.1935v1, Jul. 2014.

[16] G. Cohen, Honkala, Litsyn, Lobstein, "Covering Codes," Elsevier Science, North-Holland, 1997.

[17] P. Delsarte, "Four Fundamental Parameters of a Code and Their Combinatorial Significance," Inform. and Contl, 23, pp. 407-438, 1973.

[18] P. Delsarte, "Bilinear Forms Over a Finite Field with Applications to Coding Theory," Journal of Combinatorial Theory Series A, 1978 25, 3, pp.226-241

[19] J. de la Cruz, E. Gorla, H. H. Lopez, A. Ravagnani, "Rank Distribution of Delsarte Codes," arXiv: 1510.01008, 2015.

[20] J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems, "Algebraic Structures of MRD Codes," to appear in Advances in the Mathematics of Communications, arXiv:1502.02711.

[21] M. Dai, K. W. Shum, C. W. Sung, "Data Dissemination With Side Information and Feedback," IEEE Transactions on Wireless Communications, Vol. 13, 9, pp. 4708–4720, 2014.

[22] S. H. Dau, V. Skachek, and Y. M. Chee, "On the Security of Index Coding With Side Information", IEEE Transactions on Information Theory, vol.58, no.6, June 2012, pp. 3975–3988.

[23] S. H. Dau, V. Skachek, and Y. M. Chee, "Error Correction for Index Coding With Side Information", IEEE Transactions on Information Theory, Vol. 59 , Issue: 3, pp. 1517 - 1531, 2013.

[24] T. Etzion, "A New Approach to Examine $q$-Steiner Systems," arXiv:1507.08503, 2015.

[25] T. Etzion, " Problems on q-Analogs in Coding Theory," preprint arXiv:1305.6126

[26] M. Effros, S. El Rouayheb, M. Langberg, "An Equivalence Between Network Coding and Index Coding," IEEE Transactions on Information Theory, (61), No. 5, pp. 2478–2487, 2015.

[27] T. Etzion, E. Gorla, A. Ravagnani, A. Wachter-Zeh, "Optimal Ferrers Diagram Rank-Metric Codes,"IEEE Transactions on Information Theory, Vol. 62, No. 4, 2016, pp. 1616-1631.

[28] T. Etzion and N. Silberstein,"Error-Correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams," IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 29092919, 2009.

[29] T. Etzion and N. Silberstein: "Codes and Designs Related to Lifted MRD Codes Information Theory, IEEE Transactions on 59, 2, pp. 1004-1017, 2012.

[30] T. Etzion, A. Vardy, "Error-Correcting Codes in Projective Space," IEEE Trans on Inform. Thy, Volume 57, Issue 2, 2011.

[31] A. El Rouayheb, A. Sprintson, and C. Georghiades, "On the Index Coding Problem and its Relation to Network Coding and Matroid Theory", IEEE Transactions on Information Theory, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.

[32] A. Fazeli, S. Lovett, A. Vardy, "Nontrivial $t$-Designs over Finite Fields Exist for all $t$," Journal of Combinatorial Thory, Series A, Volume 127, Issue 1, pp. 149160, 2014.

[33] E Gabidulin, "Theory of Codes with Maximum Rank Distance," Problems of Information Transmission, 21:1, pp. 1-12, 1985.

[34] E. Gorla, A. Ravagnani, "Subspace Codes From Ferrers Diagrams," to appear in Journal of Algebra and Its Applications (see arXiv:1405.2736).

[35] M. Gadouleau, Z. Yan, "Packing and Covering Properties of Rank Metric Codes," IEEE Trans. Inform. Theory, 54 (9) 2008.

[36] M. Gadouleau, Z. Yan, "MacWilliams Identity for Codes with the Rank Metric," EURASIP Journal on Wireless Communications and Networking, Volume 2008, Issue 1, 2008.

[37] M. Gadouleau, Z. Yan, "Packing and Covering Properties of Subspace Codes for Error Control in Random Linear Network Coding,", IEEE Trans. Inform. Theory, 56 (5), pp. 2097-2108, 2010

[38] V. Guruswami, C. Wang; C. Xing, "Explicit List-Decodable Rank-Metric and Subspace Codes via Subspace Designs," IEEE Transactions on Information Theory, Vol. 62, 5, pp. 2707 - 2718, 2016

[39] X. Huang; S. El Rouayheb, "Index Coding and Network Coding via Rank Minimization," IEEE Information Theory Workshop (ITW), pp.14–18, 2015.

[40] D. Heinlein, M. Kiermaier, S. Kurz, A. Wassermann, "Tables of Subspace Codes," http://subspacecodes.uni-bayreuth.de/, arXiv preprint arXiv:1601.02864, 2016

[41] T. Honold, M. Kiermaier, "On Putative $q$-Analogues of the Fano plane and Related Combinatorial Structures," Dynamical Systems, Number Theory and Applications, pp. 141-175, 2016.

[42] A. Horlemann-Trautmann, K. Marshall, "New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions," to appear in Advances in Mathematics of Communications, 2016 (arXiv: 1507.08641).

[43] R. Kötter, F. Kschischang, "Coding for Erasures and Errors in Random Network Coding," IEEE Transactions on Information Theory, (54), 8, 2008.

[44] M. Kieremaier, S. Kurz, A. Wassermann, "The Order of the Automorphism Group of a Binary q-Analog of the Fano Plane is at Most Two," European J. Combin. 51, pp. 443457, 2016.

[45] R. Koetter, and M. Medard, "An Algebraic Approach to Network Coding", IEEE/ACM Trans. Netw., 11 (5) pp. 782-795, 2003.

[46] M. Kieremaier, M. O. Pavcević, "Journal of Combinatorial Designs 23, pp. 463-480, 2015.

[47] P. Loidreau, "A Welch-Berlekamp Like Algorithm for Decoding Gabidulin Codes," Lect. Notes in Comp. Sc., pp. 36-45, 2006.

[48] P. Loidreau, "Designing a Rank Metric Based McEliece Cryptosystem," Post-Quantum Cryptography, Lecture Notes in Computer Science Volume 6061 pp. 142-152, 2010.

[49] N. Lee, A. G. Dimakis, and R. W. Heath, Jr., "Index Coding With Coded Side-Information," IEEE Comm. Letters, 19 (3), 2015.

[50] R. Lidl, H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*, 2nd Edition, Cambridge Univ. Press, 1997.

[51] K. Morrison, "Equivalence for Rank-metric and Matrix Codes and Automorphism Groups of Gabidulin Codes," IEEE Trans. Inform. Theory 60 (11), 2014.

[52] M. Maddah-Ali, U. Niesen. "Fundamental limits of caching," IEEE Transactions on Information Theory 60.5 (2014): 2856-2867.

[53] A. Neri, A. Horlemann-Trautmann, T. Randrianarisoa, J. Rosenthal, "On the Genericity of Maximum Rank Distance and Gabidulin Codes, preprint arvix, arXiv:1605.05972v1, 2016.

[54] G. Nebe, W. Willems, "On Self-Dual MRD Codes," arXiv: 1505.07237, 2015.

[55] O. Ore, "On a Special Class of Polynomials," Trans. Amer. Math. Soc. 35 (1933) 559-584.

[56] A. Ravagnani, "Rank-Metric Codes and Their Duality Theory," Designs Codes and Cryptography, Vol. 80, Issue 1, 2016.

[57] J. Sheekey, "A New Family of MRD Codes," to appear in Adv. in Math. of Comms (see arXiv:1504.01581) 2016.

[58] K. Shanmugan, A. Dimakis, M. Langberg, "Graph Theory versus Minimum-Rank for Index Coding", Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT) (full-paper at arXiv:1402.3898.v1, Feb 2014), pp. 291-295, 2014.

[59] A. Shishkin, E. Gabidulin and N. Pilipchuk, "On Cardinality of Network Subspace Codes," Proceeding of the Fourteenth Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XIV), 7, 2014.

[60] D. Silva, F. R. Kschischang, R. Koetter, "Communication Over Finite-Field Matrix Channels", IEEE Trans. Inf. Theory, vol. 56, no. 3, pp. 1296–1305, Mar. 2010.

[61] D. Silva, F. Kschischang, R. Kötter, "A Rank-Metric Approach to Error Control in Random Network Coding," IEEE Trans. Inform. Th. (54), 9, 2008.

[62] K. W. Shum, D. Mingjun, C. Sung, "Broadcasting with Coded Side Information", 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), vol. 89, no. 94, pp. 9–12, Sept. 2012.

[63] N. Silberstein, A. Trautmann, " Subspace Codes Based on Graph Matchings, Ferrers Diagrams, and Pending Blocks," IEEE Trans. Inf. Theory, vol. 61, no. 7, pp. 3937–3954, 2015.

[64] S. Thomas, "Designs over Finite Fields," Geom. Dedicata, 21, pp. 237242, 1987.

[65] S. Thomas, "Designs and Partial Geometries over Finite Fields," Geom. Dedicata, 63, pp. 247253, 1996.

[66] C. Tian and J. Chen, "Caching and Delivery via Interference Elimination," arXiv preprint 1604.08600, 2016.

[67] A. S. Tehrani, A. G. Dimakis, M. J. Neely, "Bipartite Index Coding," Proceedings of the IEEE 2012 International Symposium on Information Theory (ISIT), Boston, Jul 1-6, 2012, pp. 2246-2250.

[68] J. I. Tamir, E. R. Elenberg, A. Banerjee, S. Vishwanath, "Wireless Index Coding Through Rank Minimization," IEEE ICC 2014 - Wireless Communications Symposium, pp. 5209-5214.

[69] J. H. van Lint and R. M. Wilson, A Course in Combinatorics. Cambridge, U.K.: Cambridge Univ. Press, 1992.

[70] K. Wan, D. Tuninetti, and P. Piantanida. "On the optimality of uncoded cache placement," arXiv preprint arXiv:1511.02256, 2015.

[71] A. Wachter-Zeh, "Bounds on List Decoding of Rank-Metric Codes," IEEE Trans. Inf. Theory, 59 (11) pp. 7268-7278, 2013.

[72] J. Zumbrägel, "Designs and Codes in Affine Geometry," arXiv preprint arXiv:1605.03789, 2016.