Hybrid Noncoherent Network Coding

Vitaly Skachek[1]
McGill University
3480 University Street
Montréal, QC H3A 2A7, Canada

Olgica Milenkovic
UIUC
1308 W. Main Street
Urbana, IL 61801, USA

Angelia Nedić
UIUC
1308 W. Main Street
Urbana, IL 61801, USA

***Abstract*—We describe a novel extension of subspace codes for noncoherent networks, suitable for use when the network is viewed as a communication system that introduces both dimension and symbol errors. We show that when symbol erasures occur in a significantly large number of different basis vectors transmitted through the network and when the min-cut of the networks is much smaller then the length of the transmitted codewords, the new family of codes outperforms their subspace code counterparts.**

For the proposed coding scheme, termed hybrid network coding, we derive two upper bounds on the size of the codes. These bounds represent a variation of the Singleton and of the sphere-packing bound. We show that a simple concatenated scheme that represents a combination of subspace codes and Reed-Solomon codes is asymptotically optimal with respect to the Singleton bound. Finally, we describe two efficient decoding algorithms for concatenated subspace code.

I. Introduction

It was suggested in [8] to use subspace coding for error correction, when the network topology is not known, or when it changes with time. In that scheme, the errors are modeled as **dimension gains** and **dimension losses**. These notions, although of theoretical value, may appear rather abstract in certain networking applications, where packets (symbols or collections of symbols) are subjected to erasures or substitution errors.

We propose **a hybrid approach** to noncoherent network coding, which attempts to connect the notions of dimension loss and gain with those of individual symbol errors and erasures. The crux of our approach is to consider network coding where dimension gains and losses, in addition to individual symbol errors and erasures, are all possible. This allows us to study the trade-offs between the required overhead in the network layer aimed at correcting dimension gains/losses, and the overhead in the physical layer designated to correcting symbol erasures and errors.

Our main result shows that by incorporating symbol error correcting mechanism into subspace codes, one can increase the number of tolerable dimension gains and losses, without compromising the network throughput. Hence, the proposed approach leads to an increase in the overall number of correctable errors in the subspace-based scheme akin to [8].

[1]The work of this author was done while he was with the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign.

This work is supported by the NSF Grants CCF0809895, CCF0821910, CCF1117980 and the Air Force Grant AF FA95500910612.

There are various potential applications for hybrid network codes [6]. Hybrid codes can be useful in networks where no link-layer error correction is performed. Such networks include sensor networks for which the computational power of intermediate nodes is not sufficiently large. This prevents error correction to be performed before the errors propagate through the network. Hybrid codes can also be used in networks for which a physical layer packet is very small, the network layer packet consists of many physical layer packets, and where the packet can be regarded as a single symbol. In this case, if an error in the physical layer packet cannot be decoded, a symbol error is declared.

II. Notation and Prior Work

Let W be a vector space over a finite field $\mathbb{F}_q$. We use the notation $\dim(W)$ for the dimension of W. For a set of vectors $S \subseteq W$, we use $\langle S \rangle$ to denote the linear span of the vectors in S. We also use the notation $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_\ell \rangle$ for a vector span of the set of vectors $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_\ell\}$. Let $\mathbb{N}$ be the set of the positive integer numbers. We write $\mathbf{0}^m$ to denote the all-zero vector of length m, for any $m \in \mathbb{N}$. When the value of m is clear from the context, we sometimes write $\mathbf{0}$ rather than $\mathbf{0}^m$. We also denote by $\boldsymbol{e}_i \in \mathbb{F}_q^n$ a unity vector which has a one in position $i \in \mathbb{N}$ and zeros in all other positions.

Let V and U be linear subspaces of W. We denote the sum of U and V as $U + V = \{\boldsymbol{u} + \boldsymbol{v} \ : \ \boldsymbol{u} \in U, \boldsymbol{v} \in V\}$. If $U \cap V = \{\mathbf{0}\}$, then for any $\boldsymbol{w} \in U + V$ there is a unique representation in terms of the sum of two vectors $\boldsymbol{w} = \boldsymbol{u} + \boldsymbol{v}$, where $\boldsymbol{u} \in U$ and $\boldsymbol{v} \in V$. In this case we say that $U + V$ is a direct sum, and denote it by $U \oplus V$. It is easy to check that $\dim(U \oplus V) = \dim(U) + \dim(V)$. Let $W = U' \oplus U''$. For $V \subseteq W$ we define a projection of V onto U', denoted by $V|_{U'}$, as follows:

$$V|_{U'} = \{\boldsymbol{u}_1 \ : \ \boldsymbol{u}_1 + \boldsymbol{u}_2 \in V, \ \boldsymbol{u}_1 \in U', \ \boldsymbol{u}_2 \in U''\} \ .$$

Similarly, we denote the projection of the vector $\boldsymbol{u}$ onto U' by $(\boldsymbol{u})|_{U'}$. For two vectors, $\boldsymbol{u}$ and $\boldsymbol{v}$, we write $\boldsymbol{u} \cdot \boldsymbol{v}$ to denote their scalar product. If $W = U' \oplus U''$ and for all $\boldsymbol{u} \in U'$, $\boldsymbol{v} \in U''$ it holds $\boldsymbol{u} \cdot \boldsymbol{v} = 0$ (i.e. U' and U'' are orthogonal), we also write $W = U' \bigodot U''$.

Assume that $\dim(W) = n$. We use the notation $\mathcal{P}(W, \ell)$ for the set of all subspaces of W of dimension ℓ, and $\mathcal{P}(W)$ for the set of all subspaces of W of any dimension. The number of ℓ-dimensional subspaces of W, $0 \leq \ell \leq n$, is given by the

q-ary Gaussian coefficient (see [14, Chapter 24]):

$$|\mathcal{P}(W,\ell)| = \begin{bmatrix} n \\ \ell \end{bmatrix}_q = \prod_{i=0}^{\ell-1} \frac{q^{n-i}-1}{q^{\ell-i}-1} \ .$$

For $U, V \in W$,

$$\mathsf{D}(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

is a distance measure between U and V in the Grassmanian metric (see [8]). We use the notation $\mathsf{d}(\boldsymbol{u},\boldsymbol{v})$ for the Hamming distance between two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ of the same length.

We say that the code $\mathbb{C}$ is an $[n,\ell,\log_q(M),D]_q$ subspace code, if it is represents a collection of subspaces in an ambient space W over $\mathbb{F}_q$, which satisfies the following conditions:

1) W is a vector space over $\mathbb{F}_q$ and $\dim(W) = n$;
2) for all $V \in \mathbb{C}$, $\dim(V) = \ell$;
3) $|\mathbb{C}| = M$;
4) for all $U, V \in \mathbb{C}$, $U \neq V$, it holds that $\dim(U \cap V) \leq \ell - D$, so that consequently $\mathsf{D}(U,V) \geq 2D$.

In [15] and [8], the subspace code $\mathcal{K}$ with parameters $[\ell + m, \ell, mk, \geq 2(\ell-k+1)]_q$ was presented, where $k \leq \ell \leq m$.

Lemma II.1. *Let $W = U' \oplus U''$ be a vector space over $\mathbb{F}_q$, and let $V_1, V_2 \subseteq W$ be two vector subspaces. Then*

$$\mathsf{D}(V_1,V_2) \geq \mathsf{D}(V_1|_{U'}, V_2|_{U'}) \ .$$

III. Hybrid Coding for Symbol Erasures and Dimension Gains/Losses

A. Motivation

Let $W_{\mathcal{L}}$ denote the space $\mathbb{F}_q^n$ for some $n \in \mathbb{N}$ and let $\mathcal{L}$ be a collection of subspaces of $W_{\mathcal{L}}$ of dimension ℓ. Assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network. Assume also that ρ symbol errors and μ symbol erasures happened to any of the vectors of V, while they were propagating through the network. Denote by U the subspace spanned by the vectors obtained at the destination.

Then, the vectors observed by the receiver are linear combinations of the vectors in V. Each of these vectors has, in the worst case scenario, at most ρ symbol errors and μ symbol erasures. Indeed, this can be justified as follows. If some vector $\boldsymbol{x}$ was transmitted in the network, and an erasure (or error) occurred in its j-th entry, in the worst case scenario this erasure (error) can effect only the j-th coordinates in *all* vectors in U, causing this coordinate to be erased (or altered, respectively) in all of them. This is true for any network topology. Such erasure (or error) does not effect any other entries in the vectors observed by the receiver.

This observation motivates the following definitions.

Definition III.1. *Consider a vector space $U \subseteq W_{\mathcal{L}}$. Write $W_{\mathcal{L}} = W_S \bigodot \langle \boldsymbol{e}_j \rangle$ for some $1 \leq j \leq n$ and for some subspace W_S. A* **symbol error** *in coordinate j of U is a mapping from U to $U' \subseteq W_{\mathcal{L}}$, such that $U \neq U'$ and $U|_{W_S} = U'|_{W_S}$.*

Definition III.2. *Let $U \subseteq W_{\mathcal{L}}$ and assume that $W_{\mathcal{L}} = W_S \bigodot \langle \boldsymbol{e}_j \rangle$ for some $1 \leq j \leq n$ and for some subspace W_S. A* **symbol erasure** *in coordinate j of U is a mapping from U to $U' \subseteq W_S$, such that $U|_{W_S} = U'$.*

Observe, that symbol errors and erasures can be combined. There are four potential types of data errors in a network that are not necessarily incurred independently:

1) Symbol erasures;
2) Symbol errors;
3) Dimension losses;
4) Dimension gains.

B. Code Definition

We start the development with the following definition.

Definition III.3. *A subspace code $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}},\ell)$ (a collection of subspaces in $W_{\mathcal{L}}$ of dimension ℓ) is called a* **code correcting** $d-1$ **symbols erasures and** $D-1$ **dimension errors** *or a (d,D)* **hybrid code** *if it satisfies the following properties:*

1) *For any $U \in \mathcal{L}$, $\dim(U) = \ell$.*
2) *For any $U, V \in \mathcal{L}$, $\dim(U)+\dim(V)-2\dim(U \cap V) \geq 2D$.*
3) *Let $V \in \mathcal{L}$. Let V' be the subspace obtained from V by μ symbol erasures, where $\mu \leq d-1$. Then, for any possible combination of μ symbol erasures with $\mu \leq d-1$, $\dim(V') = \ell$ and the space V is the only pre-image of V' in $\mathcal{L}$ (under μ symbol erasures).*
4) *Let $U, V \in \mathcal{L}$. Let U', V' be obtained from U and V, respectively, by μ symbol erasures, where $\mu \leq d-1$ (here both U and V have erasures in the same set of coordinates). Then, $\dim(U') + \dim(V') - 2\dim(U' \cap V') \geq 2D$.*

Observe that condition (1) is a special case of condition (3), and (2) is a special case of condition (4), and therefore the first two conditions can be omitted.

Theorem III.1. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}},\ell)$ be a code satisfying (1)-(4). Then, $\mathcal{L}$ is capable of correcting any error pattern of $d-1$ symbol erasures and $D-1$ dimension errors.*

Henceforth, we use the notation $[n,\ell,\log_q(M),2D,d]_q$[1] to denote the subspace code $\mathcal{L} \subseteq \mathcal{P}(W,\ell)$ with the following properties:

1) $\dim(W) = n$;
2) for all $V \in \mathcal{C}$, $\dim(V) = \ell$;
3) $|\mathcal{L}| = M$;
4) $\mathcal{L}$ is a code capable of correcting $d-1$ symbols erasures and $D-1$ dimension errors.

IV. Bounds on the Parameters of Hybrid Codes

In this section, we develop the Singleton and the sphere-packing bound for hybrid codes handling dimension losses and gains, and symbol erasures simultaneously.

[1] Whenever it is apparent from the context, we omit the subscript q.

A. Singleton Bound

Assume that a vector space W over $\mathbb{F}_q$ has dimension n, and let $\mathcal{L} \subseteq \mathcal{P}(W, \ell)$ be a subspace code. In what follows, we use a puncturing of the code $\mathcal{L}$, which is similar to symbol erasure in all $V \in \mathcal{L}$, but has a different assumption on the receiver's knowledge. Specifically, we use the following definition.

Definition IV.1. *Puncturing of the code $\mathcal{L}$ at position j is equivalent to the definition of erasure at coordinate j in Definition III.2. The only difference is that in Definition III.2 it is assumed that the receiver knows which coordinate was erased, while in this context no such knowledge is assumed.*

Theorem IV.1. *Let $\mathcal{L}$ be a code of type $[n, \ell, \log_q(M), 2D, d]$ in the ambient space $W_{\mathcal{L}}$. If $d > 1$, then coordinate puncturing at coordinate j yields a code with parameters $[n-1, \ell, \log_q(M), 2D, \geq d-1]$.*

Theorem IV.2. *The size M of the $[n, \ell, \log_q(M), 2D, d]_q$ code $\mathcal{L}$ satisfies*

$$M \leq \mathcal{A}_q(n-d+1, \ell, 2D) \ ,$$

where $\mathcal{A}_q(n, \ell, 2D)$ stands for the size of the largest subspace code $[n, \ell, M', 2D]_q$.

Proof: We apply $d-1$ coordinate puncturings to $\mathcal{L}$. The resulting code has the same number of codewords as $\mathcal{L}$, and it is a set of ℓ dimensional subspaces in a $n-d+1$ dimensional space, whose pairwise intersection is of dimension $\leq \ell - D$. In particular, its size is upper bounded by $\mathcal{A}_q(n-d+1, \ell, 2D)$. ∎

Definition IV.2. *The* **rate** *of the subspace code $\mathcal{L}$ is defined as $R = \frac{\log_q(|\mathcal{L}|)}{n\ell}$.*

Next, let

$$\lambda = \frac{\ell}{n}, \ \Delta = \frac{D}{\ell} \text{ and } \delta = \frac{d}{n} \ .$$

An asymptotic version of the latter bound is as follows.

Corollary IV.3. *The rate of the $[n, \ell, \log_q(|\mathcal{L}|), D, d]_q$ code $\mathcal{L}$ satisfies*

$$R \leq \left(1 - \Delta - \frac{1}{n}\right)\left(1 - \delta - \lambda + \frac{1}{n}\right) + o(1) \ .$$

B. Sphere-Packing Bound

Let $W_{\mathcal{L}}$ be ambient space $\mathbb{F}_q^n$, and let $0 \leq \ell \leq n$. Fix two integers $T \in [0, n]$, and $t \in [0, n]$. Two vector spaces $U, V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ are called (T, t)-*adjacent* if there exists a set of coordinates $S = \{i_1, i_2, \cdots, i_s\} \subseteq [n]$, $s \leq t$, and a vector space W_S such that

$$W_{\mathcal{L}} = W_S \bigodot \langle \boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \cdots, \boldsymbol{e}_{i_s} \rangle \ ,$$

and

$$\mathsf{D}(U|_{W_S}, V|_{W_S}) \leq T \ .$$

Note that the adjacency relation is symmetric with respect to the order of U, V, namely U and V are (T, t)-adjacent if and only if V and U are (T, t)-adjacent.

Assume that the code $\mathcal{L}$ is used over the network. Let $U_1 \in \mathcal{L}$ be transmitted, and let the space $V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ be received as a result of T dimension erasures or gains, and t coordinate erasures. Then, U_1 and V are (T, t)-adjacent. If there is no other codeword $U_2 \in \mathcal{L}$ such that U_2 and V are (T, t)-adjacent, then the decoder, which is able to correct t coordinate erasures and T dimension erasures/gains, can recover U_1 from V.

Definition IV.3. *Let $W_{\mathcal{L}}$ be the vector space $\mathbb{F}_q^n$, and let $V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$. The sphere $\mathcal{S}(V, \ell, T, t)$ around V is defined as*

$$\mathcal{S}(V, \ell, T, t) = \{U \in \mathcal{P}(W_{\mathcal{L}}, \ell) \ : \ V, U \text{ are } (T, t)\text{-adjacent}\} \ .$$

Theorem IV.4. *Let $\mathcal{L}$ be a $[n, \ell, \log_q|\mathcal{L}|, D, d]_q$ code. For any $V \in \mathcal{L}$, any $0 \leq T \leq 2\ell$ and any $0 \leq t < d$,*

$$|\mathcal{S}(V, \ell, T, t)| \geq \sum_{s=0}^{t} \binom{n}{s} \cdot \sum_{i=0}^{T/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n-s-\ell \\ i \end{bmatrix} \ .$$

From Theorem IV.4, the following sphere-packing-type bound is obtained.

Corollary IV.5. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ be a code that corrects $d-1$ symbol erasures and $D-1$ dimension losses/gains. Then*

$$|\mathcal{L}| \leq \frac{\begin{bmatrix} n \\ \ell \end{bmatrix}}{\sum_{s=0}^{d-1} \binom{n}{s} q^{\ell s} \cdot \sum_{i=0}^{(D-1)/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n-s-\ell \\ i \end{bmatrix}} \ . \tag{1}$$

The next bound is an asymptotic counterpart of (1):

$$|\mathcal{L}| \ \dot{\leq} \ 4q^{\ell(n-d-\ell+1) - nh_2((d-1)/n)\log_q 2 - (D-1)(n-d-D+2)} \ ,$$

where $h_2(x)$ denotes the binary entropy function, and $f(x) \dot{\leq} g(x)$ means that $f(x)$ is asymptotically bounded from above by $g(x)$.

By taking base-q logarithm and dividing by ℓn, we obtain the following result.

Corollary IV.6. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ be a code that corrects $d-1$ symbol erasures and $D-1$ dimension losses/gains. Then, its rate satisfies:*

$$R \leq \left(1 - \delta - \lambda + \frac{1}{n}\right) - \left(\Delta - \frac{1}{\ell}\right)\left(1 - \delta - \lambda\Delta + \frac{2}{n}\right) - \left(1 - h_2\left(\delta\lambda - \frac{1}{n}\right)\right)\frac{\log_q 2}{\ell} + o(1) \ .$$

V. Hybrid Code

A. Code Construction

Denote by W the vector space $(\mathbb{F}_q)^{m+\ell}$, and let $\mathbb{C}$ be a set of subspaces of W of dimension ℓ, such that for any $U, V \in \mathbb{C}$, $V \neq U$, $\dim(U \cap V) \leq \ell - D$. We fix a basis of W, and denote its vectors by $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_{m+\ell}\}$. We denote the decoder for the subspace metric and $\mathbb{C}$ by $\mathcal{D}_{\mathbb{C}}$.

Let $\boldsymbol{G}$ be a $(\ell+m) \times n$ generator matrix of the $[n, \ell+m, d]$ Generalized Reed-Solomon (GRS) code $\mathcal{C}$ over $\mathbb{F}_q$ of length $n \triangleq \ell + m + d - 1$ (see [9, Chapter 5] for more details).

We use the notation $\boldsymbol{G}_i$ for the i-th row of $\boldsymbol{G}$, for $i = 1, 2, \cdots, \ell+m$. The code $\mathcal{C}$ is capable of correcting any error

pattern of ρ errors and μ erasures given that $2\rho + \mu \leq d - 1$. In this section, we are particularly interested in the case when $\rho = 0$.

Denote by $\mathcal{D}_{RS}$ the decoder for the code $\mathcal{C}$. Consider a field $\mathbb{F}_{q^n}$, which can also be viewed as a vector space $(\mathbb{F}_q)^n$, denoted by $W_{\mathcal{L}}$. Let $\boldsymbol{A}$ be an $(\ell + m) \times (\ell + m)$ matrix over $\mathbb{F}_q$ such that

$$\forall i = 1, 2, \cdots, \ell + m \ : \ \boldsymbol{e}_i = \boldsymbol{u}_i \boldsymbol{A} \ ,$$

and therefore

$$\forall i = 1, 2, \cdots, \ell + m \ : \ \boldsymbol{G}_i = \boldsymbol{u}_i \boldsymbol{A} \boldsymbol{G} \ .$$

We define a linear mapping $\mathcal{E}_{\mathcal{L}} : W \to W_{\mathcal{L}}$ as follows. For an arbitrary vector $\boldsymbol{v} \in W$, $\mathcal{E}_{\mathcal{L}}(\boldsymbol{v}) = \boldsymbol{v}\boldsymbol{A}\boldsymbol{G}$. This mapping, with a slight abuse of notation, can naturally be extended to the mapping $\mathcal{E}_{\mathcal{L}} : \mathcal{P}(W) \to \mathcal{P}(\mathcal{C})$, where $\mathcal{P}(\mathcal{C})$ stands for a set of all linear sub-codes of $\mathcal{C}$. For any $V \in \mathcal{P}(W)$, we have $\mathcal{E}_{\mathcal{L}}(V) \triangleq \{\boldsymbol{v}\boldsymbol{A}\boldsymbol{G} \ : \ \boldsymbol{v} \in V\}$.

It is easy to see that $\mathcal{E}_{\mathcal{L}}$ is a linear mapping, and that the image of the linear space V is a linear space. Moreover, it is straightforward to show that this mapping, when applied to subspaces of W, is one-to-one. Thus, for any $V \in W$,

$$\dim(V) = \dim(\mathcal{E}_{\mathcal{L}}(V)) \ . \tag{2}$$

One can check that for any $U, V \in W$, there holds

$$\dim(U \cap V) = \dim(\mathcal{E}_{\mathcal{L}}(U) \cap \mathcal{E}_{\mathcal{L}}(V)) \ . \tag{3}$$

Next, we define a code $\mathcal{L} \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ as $\mathcal{L} = \{\mathcal{E}_{\mathcal{L}}(V) \ : \ V \in \mathbb{C}\}$.

Theorem V.1. *The code $\mathcal{L}$ is a hybrid code over $\mathbb{F}_q$, with parameters $[n, \ell, |\mathbb{C}|, \geq 2D, \geq d]$.*

Corollary V.2. *Let V be a subcode of $\mathcal{C}$ (of any dimension). Let V' be obtained from V by arbitrary μ symbol erasures, such that $\mu \leq d-1$. Then, $\dim(V') = \dim(V)$ and the space V is the only pre-image of V' in $\mathcal{P}(\mathcal{C})$.*

B. Asymptotic Optimality

Consider the code $\mathcal{L}$ constructed from the subspace code with parameters $[m + \ell, \ell, \log_q |\mathbb{C}|, 2D]_q$ and a classical GRS code with parameters $[n, m + \ell, d]_q$, $n = \ell + m + d - 1$, as described in the previous section. The resulting code $\mathcal{L}$ is a $[n, m + \ell, \log_q |\mathbb{C}|, 2D, d]_q$ code. The number of codewords of the code is $|\mathbb{C}|$. If we take $|\mathbb{C}|$ as described in [8], then the q-ary logarithm of the number of the codewords is given by $\log_q |\mathbb{C}| = m(\ell - D + 1)$. This code is asymptotically order-optimal (i.e., optimal up to a constant factor) with respect to the Singleton bound.

C. Examples: Hybrid versus Subspace Codes

We show the advantage of using the code $\mathcal{L}$ over $\mathcal{K}$ in the case where all data errors in the noncoherent network take form of symbol erasures. Each symbol erasure can be the cause of dimension loss. In this case, the code $\mathcal{L}$ has more codewords than $\mathcal{K}$ while having the same overall error-correcting capability. The advantage of the new construction is significantly more pronounced when the gap between ℓ and m is large.

Example V.1. Take the code $\mathcal{K}$ with parameters $[m + \ell, \ell, mk, 2(\ell - k + 1)] = [12, 4, 16, 6]_q$. This code can correct up to and including two dimension losses and it contains q^{16} codewords.

For comparison, take $W = (\mathbb{F}_q)^{10}$ and consider the set $\mathcal{P} = \mathcal{P}(W, 4)$, where $|\mathcal{P}| = \begin{bmatrix} 10 \\ 4 \end{bmatrix}_q$. Fix some basis $\{\boldsymbol{u}_i\}_{i=1}^{10}$ for $\mathcal{P}$. Let $\mathcal{C}$ be a $[12, 10, 3]_q$ GRS code, with $q \geq 11$. Define the mapping $\mathcal{E}_{\mathcal{L}} : W \to \mathcal{C}$ as before.

The resulting code $\mathcal{L}$ has parameters $[12, 4, \log_q \left(\begin{bmatrix} 10 \\ 4 \end{bmatrix}_q \right), \geq 2, 3]_q$. Since $\mathcal{C}$ has a minimum distance 3, $\mathcal{L}$ can correct any two symbol erasures.

The number of codewords in the code equals

$$\begin{bmatrix} 10 \\ 4 \end{bmatrix}_q = \frac{(q^{10} - 1)(q^9 - 1)(q^8 - 1)(q^7 - 1)}{(q^4 - 1)(q^3 - 1)(q^2 - 1)(q - 1)} > q^{24}.$$

This number is strictly larger than $4q^{16}$ (for all $q \geq 11$), which is an upper bound on the size of any $[12, 4, 16, 6]_q$ subspace code [8].

The examples described above motivate the following question: how many symbol erasures should be counted towards one dimension loss for the case that the subspace and hybrid codes have the same number of codewords?

To arrive at the desired result, we use an upper bound on the size of $\hat{\mathcal{L}}$, which was derived in [8]. Therefore, our findings are also valid for the codes constructed in [8], [12], [1], as well as for any other subspace code.

Let us fix the values of the parameters n and ℓ. Any subspace code $\hat{\mathcal{L}}$ is capable of correcting $\tilde{D} - 1$ dimension losses, so in the worst case scenario, it can provably correct only up to $\tilde{D} - 1$ symbol erasures. From [8, Theorem 9] we have

$$|\hat{\mathcal{L}}| \leq \begin{bmatrix} n - \tilde{D} + 1 \\ \ell - \tilde{D} + 1 \end{bmatrix}_q < 4q^{(\ell - \tilde{D} + 1)(n - \ell)} \ .$$

In comparison, the number of codewords in the code constructed in Section V-A is given by

$$|\mathcal{L}| = q^{(\ell - D + 1)(n - \ell - d + 1)} \ .$$

In order to achieve the same erasure-correcting capability, we set $\tilde{D} - 1 = (D - 1) + (d - 1)$. The underlying assumption is that $D-1$ symbol erasures are corrected as dimensional losses, while the remaining erasures are handled as simple erasures. We require that, for small $\epsilon > 0$,

$$(\ell - (\tilde{D} - 1))(n - \ell) + \epsilon < (\ell - (D - 1))(n - \ell - (d - 1)) \ , \text{ or}$$

$$(n - 2\ell + (D - 1))(d - 1) > \epsilon \ . \tag{4}$$

The latter inequality holds for any choice of $D \geq 2$ and $d \geq 2$, when $n \geq 2\ell + \epsilon'$, for some small $\epsilon' > 0$. When the inequality (4) is satisfied, hybrid codes correct more symbol erasures than any constant-dimension subspace code, designed to correct dimension errors only.

Next, we maximize the number of codewords in $\mathcal{L}$ under the constraints that $(D-1)+(d-1)=\tilde{D}-1$, and $D \geq 1$, $d \geq 1$, where $\tilde{D}$ is fixed and D, d are allowed to vary. We find that the value of d that maximizes the number of codewords equals

$$d_{opt} = \frac{n+\tilde{D}+1}{2} - \ell.$$

If $n > 2\ell$, then under the given constraints, the optimal value of d equals $d_{opt} = \tilde{D}$.

Assume that for a specific code $\mathcal{L}$, correcting a dimension loss is on average equivalent to correcting c symbol erasures, for some $\mathsf{c} > 0$.

If the error pattern consists of no dimension losses and $d-1$ symbol erasures, then q-log of the number of codewords becomes $\ell(n-\ell-(d-1))$. In comparison, if the error pattern consists of $D-1$ dimension losses and no symbol erasures, then q-log of the number of codewords becomes $(\ell-(D-1))(n-\ell)$. Since each dimension loss is on average equivalent to c symbol erasures, we have

$$(\ell-(d/\mathsf{c}-1))(n-\ell) = \ell(n-\ell-(d-1)) \ .$$

We obtain that $\mathsf{c} \approx (n-\ell)/\ell$. Therefore, vaguely speaking, it is as hard to correct one dimension loss as to correct $(n-\ell)/\ell$ symbol erasures.

VI. Decoding

We proceed to present an efficient decoding procedure which handles symbol erasures, dimension losses and dimension gains. Note that the proposed decoding method may fail in the case that symbol errors are also present. This issue is discussed in more details in Section VII.

As before, assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network. Assume also that $U \in \mathcal{P}(W_{\mathcal{L}}, \ell')$, where ℓ' is not necessarily equal to ℓ, was received.

Let U' denote the vector space U, where all erased coordinates are deleted. Similarly, let $\mathcal{C}'$ denote the code $\mathcal{C}$ where all coordinates erased in U are deleted. We first compute $\tilde{U}' = \mathcal{C}' \cap U'$, the intersection of U' with the subspace spanned by the code $\mathcal{C}'$. Assume that $\{\boldsymbol{\gamma}'_1, \boldsymbol{\gamma}'_2, \cdots, \boldsymbol{\gamma}'_{\ell''}\}$ are basis vectors of $\tilde{U}'$ (when all erased coordinates are deleted), and $\boldsymbol{\gamma}'_i \in (\mathbb{F}_q \cup \{?\})^n$. We apply the erasure-correcting GRS decoder $\mathcal{D}_{RS}$ of the code $\mathcal{C}$ on each $\boldsymbol{\gamma}'_i$ so as to obtain $\boldsymbol{\gamma}_i$. Let $\tilde{U} = \langle \boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{\ell''} \rangle$. We proceed to apply the inverse of the mapping $\mathcal{E}_{\mathcal{L}}$, denoted by $\mathcal{E}_{\mathcal{L}}^{-1}$, to $\tilde{U}$. The resulting subspace $\tilde{V}$ is a subspace of W, on which we now run the decoder for the code $\mathbb{C}$.

The algorithm described above is summarized in Figure 1.

This decoder can correct any combination of Θ dimension losses and Ω dimension gains such that $\Theta + \Omega \leq D-1$, and at most $d-1$ symbol erasures. This is stated in the following theorem.

Theorem VI.1. *The decoder in Figure 1 can correct any error pattern of up to $d-1$ symbol erasures and up to $D-1$ dimension errors in $\mathcal{L}$.*

Input: $U \subseteq (\mathbb{F}_q \cup \{?\})^n$.
Let U' be the space U, where all erased coordinates are deleted.
Let $\mathcal{C}'$ be the code $\mathcal{C}$, where all coordinates erased in U are deleted.
Let $\tilde{U}' = \mathcal{C}' \cap U'$.
Denote $\tilde{U}' = \langle \boldsymbol{\gamma}'_1, \boldsymbol{\gamma}'_2, \cdots, \boldsymbol{\gamma}'_{\ell''} \rangle$.
For $i = 1, 2, \cdots, \ell''$ **let** $\boldsymbol{\gamma}_i = \mathcal{D}_{RS}(\boldsymbol{\gamma}'_i)$.
Let $\tilde{U} = \langle \boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{\ell''} \rangle$.
Let $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.
Let $V_0 = \mathcal{D}_{\mathbb{C}}(\tilde{V})$.
Output: V_0.

Fig. 1. Decoder for dimension errors.

The time complexity of the presented decoding algorithm is bounded from above by $O\left((\ell+m)n^2 + D(\ell+m)^3\right)$ operations over $\mathbb{F}_q$.

We note that the most time-consuming step in the decoding process is decoding of a constant-dimension subspace code, which requires $O(D(m+\ell)^3)$ operations over $\mathbb{F}_q$. However, if the error pattern in a specific network contains a large number of symbol erasures, we can design the code such that D is small (say, some small constant), thus reducing the complexity of the overall decoder.

VII. Correcting Dimensions and Symbol Errors

We describe next how to use the code $\mathcal{L}$ defined in Section V-A for correction of error patterns that consist of dimension losses, symbol erasures and symbol substitutions. We show that the code $\mathcal{L}$ is capable of correcting any error pattern of up to Θ dimension losses, ρ symbol errors and μ symbol erasures, whenever $\Theta \leq D-1$ and $2\rho+\mu \leq d-1$. However, we note that if in addition to dimension losses one also encounters dimension gains, the decoder for the code $\mathcal{L}$ might fail. This issue is elaborated on in the second part of Section VII.

A. Decoding

Henceforth, we assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network and that $U \in \mathcal{P}(W_{\mathcal{L}}, \ell')$, where ℓ' is not necessarily equal to ℓ, is received.

Suppose that $\{\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{\ell'}\}$, $\boldsymbol{\gamma}_i \in (\mathbb{F}_q \cup \{?\})^n$, are some basis vectors of U. We apply the GRS decoder $\mathcal{D}_{RS}$ for the code $\mathcal{C}$ on all these vectors. This decoder produces the vectors $\{\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \cdots, \boldsymbol{\beta}_{\ell'}\} \in \mathcal{C}$. We denote by $\tilde{U}$ the span of these vectors. Then, we apply the inverse of the mapping $\mathcal{E}_{\mathcal{L}}$, denoted by $\mathcal{E}_{\mathcal{L}}^{-1}$, to $\tilde{U}$. The resulting subspace is a subspace of W, on which the decoder for the code $\mathbb{C}$ is applied.

The decoding algorithm can be summarized as in Figure 2.

Analysis of the Decoding Algorithm:

Theorem VII.1. *The decoder in Figure 2 can correct any error pattern in $\mathcal{L}$ which consists of Θ dimension losses, ρ*

Input: $U = \langle \boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{\ell'} \rangle$, $\boldsymbol{\gamma}_i \in (\mathbb{F}_q \cup \{?\})^n$.
For $i = 1, 2, \cdots, \ell'$ **let** $\boldsymbol{\beta}_i = \mathcal{D}_{RS}(\boldsymbol{\gamma}_i)$.
Let $\tilde{U} = \langle \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \cdots, \boldsymbol{\beta}_{\ell'} \rangle$.
Let $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.
Let $V_0 = \mathcal{D}_{\mathbb{C}}(\tilde{V})$.
Output: V_0.

Fig. 2. Decoder for symbol errors.

symbol errors and μ symbol erasures, whenever $\Theta \leq D - 1$ and $2\rho + \mu \leq d - 1$.

Decoding Time Complexity: The time complexity of the presented decoding algorithm is bounded from above by $O\left(Dn^3 + \ell' n^2 + \ell'^2 n\right)$ operations over $\mathbb{F}_q$.

The number of operations depends on the dimension of the received subspace, ℓ'.

B. Dimension Insertion and Decoder Failure

The following example illustrates that the decoder in Figure 2 may fail in the presence of both symbol errors and dimension gains.

Let $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_6\} \subseteq \mathbb{F}_q^6$, $q \geq 8$, be a standard basis of W, let $\ell = 3$, and let $\mathbb{C} \subseteq W$ be a subspace code with $2D = 6$. The code $\mathbb{C}$ is able to correct up to and including two dimension losses and/or gains. Additionally, let $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_6\} \in \mathbb{F}_q^8$ be a basis of a $[8, 6, 3]_q$ GRS code $\mathcal{C}$. The code $\mathcal{C}$ is able to correct one symbol error. Assume, without loss of generality, that $\boldsymbol{u}_5 = (x_1, x_2, x_3, 0, \cdots, 0) \in \mathcal{C}$ is a codeword of a minimal weight in $\mathcal{C}$.

Assume that the sender wants to transmit the space $Z = \langle \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3 \rangle$ to the receiver. According to the algorithm, the sender encodes this space as $V = \mathcal{E}_{\mathcal{L}}(Z) = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3 \rangle$, and sends the vectors $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, $\boldsymbol{u}_3$ through the network. Assume that the vector $\boldsymbol{u}_3$ is removed, and the erroneous vector $\boldsymbol{z} = \boldsymbol{u}_4 + (x_1, 0, \cdots, 0)$ is injected instead. At this point, the corresponding vector space under transmission is $\langle \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{z} \rangle$. Then, it is plausible that $\boldsymbol{u}_1$, $\boldsymbol{u}_2$ and $\boldsymbol{z}$ propagate further through the network due to network coding. To this end, assume that the receiver receives the following linear combinations, $\boldsymbol{u}_1 + \boldsymbol{z}$ and $\boldsymbol{u}_2 + \boldsymbol{z}$. Assume also that during the last transmission, the vector $\boldsymbol{z}$ is subject to a symbol error, resulting in $\boldsymbol{z}' = \boldsymbol{u}_4 + (x_1, x_2, 0, \cdots, 0)$.

The receiver applies the decoder $\mathcal{D}_{RS}$ on these three vectors, resulting in

$$\begin{aligned} \mathcal{D}_{RS}(\boldsymbol{u}_1 + \boldsymbol{z}) &= \boldsymbol{u}_1 + \boldsymbol{u}_4 \ ; \\ \mathcal{D}_{RS}(\boldsymbol{u}_2 + \boldsymbol{z}) &= \boldsymbol{u}_2 + \boldsymbol{u}_4 \ ; \\ \mathcal{D}_{RS}(\boldsymbol{z}') &= \boldsymbol{u}_4 + \boldsymbol{u}_5 \ . \end{aligned}$$

We have that

$$\tilde{U} = \langle \boldsymbol{u}_1 + \boldsymbol{u}_4, \boldsymbol{u}_2 + \boldsymbol{u}_4, \boldsymbol{u}_4 + \boldsymbol{u}_5 \rangle \ ,$$

and

$$\tilde{V} = \langle \boldsymbol{e}_1 + \boldsymbol{e}_4, \boldsymbol{e}_2 + \boldsymbol{e}_4, \boldsymbol{e}_4 + \boldsymbol{e}_5 \rangle \ .$$

Observe that $\dim(Z \cap \tilde{V}) = 1$ and that $\boldsymbol{e}_1 + \boldsymbol{e}_2 \in Z \cap \tilde{V}$, so that the subspace distance between V and $\tilde{V}$ is four. Therefore, the subspace decoder $\mathcal{D}_{\mathbb{C}}$ may fail when decoding Z from $\tilde{V}$.

VIII. Conclusion

We introduced a new class of subspace codes capable of correcting both dimension errors and symbol errors, termed hybrid codes. For these codes, we derived upper bounds on the size of the codes and presented an asymptotically constant-optimal concatenated code design method. We presented polynomial-time decoding algorithms which are capable of correcting the following error patterns:

- Dimension losses/gains and symbol erasures;
- Dimension losses and symbol erasures/errors.

We also discussed correction of error patterns that consist of all four types of errors: dimension losses/gains and symbol erasures/errors. As we illustrated by the example, the corresponding task is difficult, and is left as an open problem.

Acknowledgment: The authors are grateful to Danilo Silva for providing useful and insightful comments about the work in the manuscript. The full version of this paper is available online as `http://www.arxiv.org/1234.5678`.

References

[1] T. Etzion, N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *IEEE Trans. On Inform. Theory*, vol. 55, pp. 2909-2919, July 2009.
[2] T. Etzion, A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. On Inform. Theory*, vol. 57, pp. 1165-1173, Feb. 2011.
[3] E. M. Gabidulin, "Theory of codes with maximal rank distance," *Problems of Information Transmission*, vol. 21, pp. 1-12, July 1985.
[4] T. Ho, R. Kötter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," *Proc. IEEE Intern. Symposium on Inform. Theory (ISIT)*, Yokohama, Japan, June-July 2003.
[5] M. Jafari Siavoshani, S. Mohajer, C. Fragouli, and S. Diggavi, "On the capacity of non-coherent network coding," *IEEE Trans. On Inform. Theory*, vol. 57, no. 2, pp. 1046–1066, Feb. 2011.
[6] S. Katti, D. Katabi, H. Balakrishnan and M. Medard, "Symbol-level network coding for wireless mesh networks," *ACM SIGCOMM*, Seattle, USA.
[7] A. Khaleghi, D. Silva, and F. R. Kschischang, "Subspace codes," *Lecture Notes In Computer Science*, vol. 5921, pp. 1–21, 2009.
[8] R. Kötter, F.R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. On Inform. Theory*, vol. 54, pp. 3579–3591, Aug. 2008.
[9] R. M. Roth, *Introduction to Coding Theory*, Cambridge, UK: Cambridge University Press, 2006.
[10] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inform. Theory*, vol. 37, pp. 328-336, March 1991.
[11] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error-control in random network coding," *IEEE Trans. on Inform. Theory*, vol. 54, pp. 3951-3967, Sept. 2008.
[12] V. Skachek, "Recursive code construction for random networks," *IEEE Trans. on Inform. Theory*, vol. 56, pp. 1378-1382, March 2010.
[13] A.-L. Trautmann, J. Rosenthal, "New improvements on the echelon-Ferrers construction," *Proc. 19th Intern. Symposium on Math. Theory of Networks and Systems (MTNS)*, pp. 405–408, Budapest, Hungary, 2010.
[14] J.H. van Lint, R.M. Wilson, *A* Course in Combinatorics, Cambridge, UK: Cambridge University Press, second ed., 2001.
[15] H. Wang, C. Xing, and R. Safavi-Naini, "Linear authentication codes: bounds and constructions," *IEEE Trans. On Inform. Theory*, vol. 49, pp. 866–873, Apr. 2003.