

Distributed Storage Codes Meet Multiple-Access Wiretap Channels

Dimitris S. Papailiopoulos and Alexandros G. Dimakis

Department of Electrical Engineering

University of Southern California

Los Angeles, CA 90089

Email:{papailio, dimakis}@usc.edu

Abstract—We consider *i)* the overhead minimization of maximum-distance separable (MDS) storage codes for the repair of a single failed node and *ii)* the total secure degrees-of-freedom (S-DoF) maximization in a multiple-access compound wiretap channel. We show that the two problems are *formally* connected. Specifically, the overhead minimization for a single node failure of an *optimal* MDS code, i.e. one that can achieve the information theoretic overhead minimum, reduces to maximizing the S-DoF in a multiple-access compound wiretap channel. Additionally, we show that maximizing the S-DoF in a multiple-access compound wiretap channel reduces to minimizing the overhead of an MDS code for the repair of a departed node. An optimal MDS code maps to a full S-DoF channel and a full S-DoF channel maps to an MDS code with minimum repair overhead for one failed node. We also state a general framework for code-to-channel and channel-to-code mappings and performance bounds between the two settings. The underlying theme for all connections presented is interference alignment (IA). The connections between the two problems become apparent when we restate IA as an optimization problem. Specifically, we formulate the overhead minimization and the S-DoF maximization as rank constrained, sum-rank and max-rank minimization problems respectively. The derived connections allow us to map repair strategies of recently discovered repair codes to beamforming matrices and characterize the maximum S-DoF for the single antenna multiple-access compound wiretap channel.

I. INTRODUCTION

A substantial volume of recent work has focused on wireless interference alignment techniques [1] – [5] for wiretap channels [6] – [11]. For these settings, the high SNR secure capacity scaling or the capacity prelog factor is the S-DoF that measure the number of secure and interference free space, time, and frequency dimensions. Confining interference and wiretapped dimensions to the minimum subspace maximizes the S-DoF and achieves the high SNR secure capacity. Perfectly fulfilling this purpose, IA serves as a means to maximize the secure and interference free signaling dimensions.

Interestingly, IA was recently used in a different framework to achieve minimum overhead repair of failed storage nodes in MDS coded distributed storage systems [12] – [20]. For the repair problem that we study, a data node of the storage array fails and a newcomer takes its place to exactly regenerate the missing contents. Appropriate repair strategies are used to mix sufficient amount of the remaining data so that the newcomer downloads it and reconstructs the missing contents.

This repair process reduces to solving an underdetermined system of equations in the lost data, where the undesired file pieces generate interference to a square system of equations in the lost contents. The interference has to be subtracted and the remaining system of interest needs to be full rank. The download overhead to obtain the full rank property and erase interference is proportional to the size of the lost data plus the total number of interference dimensions. Therefore, MDS storage codes and repair strategies resulting to maximum aligned interference spaces, minimize the overhead to repair a failure in the system.

In parallel to the repair problem, we study the multiple-access compound wiretap channel. A number of non-interfering users aim to communicate with one receiver of interest, while keeping their messages secret with respect to a group of non-cooperating eavesdroppers. To maximize the perfect secrecy data rate, the beamforming strategies of each user have to be designed so that the signaling dimensions observed by the eavesdropper with the sharpest eye are minimized. That way, the number of secure links between the users and the legitimate receiver at the worst wiretapping scenario are maximized. The concept of IA comes to place when designing the beamforming strategies so that the signal spaces of the users align on top of each other causing the best eavesdropper to have access to the minimum number of communication dimensions.

Our contributions: Motivated by interference alignment that is employed in both cases [13], [19], [20], [8], and [7], we aim to formally bridge the two seemingly different settings. We establish the connection by formulating IA as a rank minimization, in the same manner as [21]: *i)* Given an MDS storage code, minimizing the overhead to exactly regenerate a failed node in the storage array is equivalent to a rank constrained, sum of ranks minimization, *ii)* for a multiple-access compound wiretap channel, the S-DoF maximization can be recast to a rank constrained, maximum-rank minimization, when the user signal spaces span all available dimensions. Then, we establish an exact reduction for the class of *optimal* MDS storage codes achieving the information theoretic minimum overhead bound of [12]. For this class of codes, the overhead minimization for the repair problem reduces to the S-DoF maximization in a class of multiple-

access compound wiretap channels. Accordingly, for a class of multiple-access compound wiretap channels, maximizing the S-DoF reduces to minimizing the overhead of an MDS code for the repair a failed node. Additional connections come in the form of code-to-channel, channel-to-code, and repair and beamforming strategy mappings. We further establish mappings and overhead or S-DoF bounds for general classes of codes or channels.

Although we provide constructive examples that validate the connection, we need to note that there is one important difference between the two problems: distributed storage problems require rank minimization *over a finite field* whereas S-DoF maximization *over the reals*. Surprisingly, the symbol extension technique [19] is applicable in both cases, for sufficiently large finite fields. The derived connection allows us to map repair strategies of recently discovered codes in [19] and [20] to beamforming matrices and characterize the maximum S-DoF for the single antenna multiple-access compound wiretap channel, extending the works of [8] and [7]. Bagherikaram et al. [8] asymptotically achieve the outer bound of $\frac{L-1}{L}$ S-DoF for L users and the single eavesdropper case, whereas Khisti [7] achieves the same bound for the L antenna MISO with multiple eavesdroppers.

II. REPAIR OF MDS STORAGE CODES

In this section, we consider the process of exactly repairing a failed node in an MDS encoded distributed storage system [14]. We show that given the code, the overhead minimization for the repair of a single node that leaves the system can be recast to a rank constrained sum of ranks minimization.

Let a file \mathbf{f} , without loss of generality be subpacketized into $M = k(n-k)\beta$ “bits” such that $\mathbf{f} \in \mathbb{F}^{k(n-k)\beta}$ and partitioned in k parts $\mathbf{f} = [\mathbf{f}_1^T \dots \mathbf{f}_k^T]^T$, with $\mathbf{f}_i \in \mathbb{F}^{(n-k)\beta}$, where M denotes the filesize in “bits” and $\beta \in \mathbb{N}^*$ the degree of subpacketization.¹ We want to store this file with rate $\frac{k}{n} \leq 1$ across k systematic and $n-k$ parity storage units with storage capacity $\alpha = \frac{M}{k}$ each. Moreover, we require to retrieve the original file by accessing any k of these n storage nodes. These redundancy and retrieval properties are achieved by using an $(n, k)_\beta$ MDS code to encode the file across the storage nodes. The encoding is given by $[\mathbf{I}_{k(n-k)\beta \times k(n-k)\beta} \mathbf{A}^T] \mathbf{f}$, where \mathbf{I}_N is the $N \times N$ identity matrix and we use

$$\mathbf{A} \triangleq \begin{bmatrix} \mathbf{A}_1^{(1)} & \dots & \mathbf{A}_1^{(n-k)} \\ \mathbf{A}_2^{(1)} & \dots & \mathbf{A}_2^{(n-k)} \\ \vdots & \vdots & \vdots \\ \mathbf{A}_k^{(1)} & \dots & \mathbf{A}_k^{(n-k)} \end{bmatrix} \in \mathbb{F}^{k(n-k)\beta \times (n-k)^2\beta} \quad (1)$$

to denote the given systematic $(n, k)_\beta$ MDS code, where $\mathbf{A}_i^{(p)} \in \mathbb{F}^{(n-k)\beta \times (n-k)\beta}$, for all $i \in \{1, \dots, k\}$ and $p \in \{1, \dots, n-k\}$. Posterior to the data encoding process k systematic storage nodes $\{1, \dots, k\}$, individually store one of the k parts of the file, $\mathbf{f}_1, \dots, \mathbf{f}_k$, respectively. Each of the

¹For distributed storage problems \mathbb{F} corresponds to a finite field; for the sake of generality we note that \mathbb{F} may represent the real numbers.

systematic node	file data
1	\mathbf{f}_1
\vdots	\vdots
k	\mathbf{f}_k
parity node	parity data
1	$(\mathbf{A}_1^{(1)})^T \mathbf{f}_1 + \dots + (\mathbf{A}_k^{(1)})^T \mathbf{f}_k$
\vdots	\vdots
$n-k$	$(\mathbf{A}_1^{(n-k)})^T \mathbf{f}_1 + \dots + (\mathbf{A}_k^{(n-k)})^T \mathbf{f}_k$

Fig. 1. STORAGE CODE

$n-k$ parity nodes $\{1, \dots, n-k\}$, stores a unique linear combination of the same k file pieces. The structure of the storage array is given in Fig. 1, where each node expends exactly $\alpha = (n-k)\beta$ worth of storage capacity. Observe that $\mathbf{A}_i^{(p)} \in \mathbb{F}^{(n-k)\beta \times (n-k)\beta}$ represents a matrix of coding coefficients used by the p th parity node to “mix” the contents of the i th file piece \mathbf{f}_i , $i \in \{1, \dots, k\}$, $p \in \{1, \dots, n-k\}$.

To maintain the same redundancy when a single systematic node fails, a repair process takes place to regenerate the lost data in a *newcomer* storage component. This process is carried out as linear operations on the contents of the $n-1$ remaining nodes. Let for example, an $(n, k)_\beta$ MDS code \mathbf{A} and a systematic node $i \in \{1, \dots, k\}$ of the array of n nodes fail. Then, a newcomer joins the storage network and we assume it connects to all $n-1$ remaining nodes that need to send it sufficient data to reconstruct \mathbf{f}_i . The repair of systematic node $i \in \{1, \dots, k\}$ can be seen as a two parallel part process. First, observe that the missing piece \mathbf{f}_i exists as a term of linear combination *only* at each parity node, as Fig. 1 shows. Carrying out one part of the repair, each parity node $p \in \{1, \dots, n-k\}$ sends a size of β data to the newcomer

$$\begin{aligned} \mathbf{y}_i^{(p)} &= (\mathbf{R}_i^{(p)})^T \left((\mathbf{A}_1^{(p)})^T \mathbf{f}_1 + \dots + (\mathbf{A}_k^{(p)})^T \mathbf{f}_k \right) \\ &= [\mathbf{A}_1^{(p)} \mathbf{R}_i^{(p)} \dots \mathbf{A}_k^{(p)} \mathbf{R}_i^{(p)}]^T \mathbf{f} \in \mathbb{F}^\beta, \end{aligned}$$

where $\mathbf{R}_i^{(p)} \in \mathbb{F}^{(n-k)\beta \times \beta}$ is the *repair matrix* that is free to design and mixes the contents of parity node p for the repair process of systematic node i , $i \in \{1, \dots, k\}$. In the same manner, all parity nodes proceed in sending a total of $(n-k)\beta$ linear equations to the newcomer. Eventually, it receives the following stack of data

$$\begin{aligned} \mathbf{y}_i &\triangleq \begin{bmatrix} (\mathbf{y}_i^{(1)})^T & \dots & (\mathbf{y}_i^{(n-k)})^T \end{bmatrix} \\ &= \begin{bmatrix} (\mathbf{A}_1^{(1)} \mathbf{R}_i^{(1)})^T & \dots & (\mathbf{A}_k^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots & \vdots & \vdots \\ (\mathbf{A}_1^{(n-k)} \mathbf{R}_i^{(n-k)})^T & \dots & (\mathbf{A}_k^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix} \mathbf{f} \\ &= \underbrace{\begin{bmatrix} (\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots \\ (\mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix}}_{\text{useful data}} \mathbf{f}_i + \sum_{u=1, u \neq i}^k \underbrace{\begin{bmatrix} (\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots \\ (\mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix}}_{\text{interference by } \mathbf{f}_u} \mathbf{f}_u, \end{aligned} \quad (2)$$

where $\mathbf{y}_i \in \mathbb{F}^{(n-k)\beta}$. Retrieving the lost piece solely from (2) is equivalent to solving an underdetermined set of $(n-k)\beta$ equations in $k(n-k)\beta$ unknowns \mathbf{f} , with respect to only the $(n-k)\beta$ unknowns of \mathbf{f}_i . However, obtaining \mathbf{f}_i is not possible due to the *interference* caused by the undesired $(k-1)(n-k)\beta$ unknowns \mathbf{f}_u , $u \in \{1, \dots, k\} \setminus i$, to the received equations, as noted in (2).

For the other part of the repair process, the newcomer needs to “erase” all interference caused by the undesired $(k-1)(n-k)\beta$ unknowns. This is possible through downloading data from the remaining systematic nodes $\{1, \dots, k\} \setminus i$ and appropriately combining them to construct exactly the sum of interference components and regenerate \mathbf{f}_i from \mathbf{y}_i through the following linear operations

$$\mathbf{f}_i = \begin{bmatrix} (\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots \\ (\mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix}^{-1} \left(\mathbf{y}_i - \sum_{u=1, u \neq i}^k \begin{bmatrix} (\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots \\ (\mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix} \mathbf{f}_u \right). \quad (3)$$

To uniquely determine \mathbf{f}_i , we require

$$\text{rank} \left(\begin{bmatrix} \mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right) = (n-k)\beta, \quad (4)$$

which is guaranteed if all equations sent by the parities are linearly independent. Surprisingly, the size of data needed to be downloaded from the systematic nodes to erase interference is not necessarily equal to the size of interfering components $(k-1) \cdot (n-k)\beta$, but depends on the level of alignment of such interference. Namely, to erase interference created by \mathbf{f}_u , we need only download from the systematic part u the smallest number of equations that can generate the interference components: a size equal the dimension of a linearly independent basis of the row span of the interference space $\begin{bmatrix} \mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix}$, $u \in \{1, \dots, k\} \setminus i$, suffices.

Consequently, the size of data needed to be downloaded from the systematic parts to erase interference, equals exactly the sum of ranks of the interference spaces

$$\sum_{u=1, u \neq i}^k \text{rank} \left(\begin{bmatrix} \mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right).$$

Therefore, for an $(n, k)_\beta$ MDS code \mathbf{A} and a certain set of repair matrices

$$\mathbf{R}_i \triangleq \begin{bmatrix} \mathbf{R}_i^{(1)} & \dots & \mathbf{R}_i^{(n-k)} \end{bmatrix} \in \mathbb{F}^{(n-k)\beta \times (n-k)^2\beta} \quad (5)$$

the overhead for exact repair of a systematic node i is defined as

$$\begin{aligned} \delta((n, k)_\beta, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) &\triangleq \frac{(n-k)\beta + \sum_{u=1, u \neq i}^k \text{rank} \left(\begin{bmatrix} \mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right)}{(n-k)\beta} \\ &= 1 + \sum_{u=1, u \neq i}^k \frac{\text{rank} \left(\begin{bmatrix} \mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right)}{(n-k)\beta}, \end{aligned} \quad (6)$$

for $i \in \{1, \dots, k\}$, where $\mathbf{P}_i \triangleq [\mathbf{E}_i \mathbf{E}_1 \dots \mathbf{E}_{i-1} \mathbf{E}_{i+1} \dots \mathbf{E}_k]$, $\mathbf{E}_i \triangleq \mathbf{e}_i \otimes \mathbf{I}_{(n-k)\beta}$, and \mathbf{e}_i corresponds to the i th column of

\mathbf{I}_k , for all $i \in \{2, \dots, k\}$. Observe that for an $(n, k)_\beta$ MDS code \mathbf{A} we have

$$\mathbf{P}_i \mathbf{A} = \begin{bmatrix} \mathbf{A}_i^{(1)} & \dots & \mathbf{A}_i^{(n-k)} \\ \mathbf{A}_1^{(1)} & \dots & \mathbf{A}_1^{(n-k)} \\ \vdots & \vdots & \vdots \\ \mathbf{A}_{i-1}^{(1)} & \dots & \mathbf{A}_{i-1}^{(n-k)} \\ \mathbf{A}_{i+1}^{(1)} & \dots & \mathbf{A}_{i+1}^{(n-k)} \\ \vdots & \vdots & \vdots \\ \mathbf{A}_k^{(1)} & \dots & \mathbf{A}_k^{(n-k)} \end{bmatrix},$$

i.e. the first row block corresponds to the set of coding matrices multiplying file piece \mathbf{f}_i , $i \in \{1, \dots, k\}$, for $i \in \{1, \dots, k\}$.

Therefore, the overhead is minimized when the *interference alignment* is maximized, i.e. when the row spans of the matrices generating the interference belong to a subspace of minimum dimension. To minimize the overhead $\delta((n, k)_\beta, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i)$, for a given $(n, k)_\beta$ MDS code \mathbf{A} , we may optimize over the repair matrices \mathbf{R}_i . This optimization can be recast to the following a rank constrained, sum of ranks minimization

$\mathcal{R}((n, k)_\beta, \mathbf{P}_i \mathbf{A})$:

$$\begin{aligned} &\min_{\mathbf{R}_i^{(1)}, \dots, \mathbf{R}_i^{(n-k)}} \sum_{u=1, u \neq i}^k \text{rank} \left(\begin{bmatrix} \mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right) \\ &\text{s.t.: } \text{rank} \left(\begin{bmatrix} \mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} & \dots & \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)} \end{bmatrix} \right) = (n-k)\beta. \end{aligned}$$

Lemma 1: For a given $(n, k)_\beta$ MDS storage code \mathbf{A} , solving $\mathcal{R}((n, k)_\beta, \mathbf{P}_i \mathbf{A})$ is equivalent to minimizing the overhead to repair node $i \in \{1, \dots, k\}$.

We note that the minimum repair overhead for a code of a given rate drastically depends on its design. Following the cut-set analysis of [12], for optimal $(n, k)_\beta$ MDS codes at the information theoretic minimum, each of the $n-1$ surviving nodes has to deliver a size of β repair data. For such MDS code structure interference spaces can align in β -dimensional subspaces, resulting in minimum repair overhead $\frac{n-1}{n-k}$.

We now shift to a seemingly unrelated problem: the S-DoF maximization of a multiple-access compound wiretap channel. Then, we establish a formal connection to the repair problem.

III. MULTIPLE-ACCESS COMPOUND WIRETAP CHANNEL

In this section, we consider a multiple-access compound wiretap channel. We show that given full rank signal spaces, the S-DoF maximization can be formulated as a rank constrained maximum rank minimization.

In the multiple-access compound wiretap channel, L users wish to communicate with a sole legitimate receiver, while maintaining message secrecy with respect to $K-1$ eavesdroppers. Each user $l \in \{1, \dots, L\}$ is equipped with M_t transmit antennas and wishes to transmit a length N symbol vector $\mathbf{x}^{(l)} \in \mathbb{R}^{N \times 1}$. We assume that the legitimate receiver and each eavesdropper v is equipped with M_r receive antennas, respectively, where $v \in \{1, \dots, K-1\}$. We further assume that $M_t = M_r = LN$. We denote such channel as an $(L, N)^{K-1}$ multiple-access compound wiretap channel. The $LN \times 1$ pulse

matched and downconverted received signals at the legitimate receiver and the v th eavesdropper are

$$\mathbf{y} = \sum_{l=1}^L \mathbf{H}^{(l)} \mathbf{V}^{(l)} \mathbf{x}^{(l)} + \mathbf{w} \quad (7)$$

$$\text{and } \mathbf{y}_{ev} = \sum_{l=1}^L \mathbf{H}_{ev}^{(l)} \mathbf{V}^{(l)} \mathbf{x}^{(l)} + \mathbf{w}_{ev}, \quad (8)$$

respectively, where $\mathbf{H}^{(l)} \in \mathbb{R}^{LN \times LN}$ represents the “channel processing” between the l th user and the receiver of interest, $\mathbf{V}^{(l)} \in \mathbb{R}^{LN \times N}$ is the beamforming matrix of user l , and \mathbf{w} accounts for zero-mean additive white Gaussian noise with covariance matrix $\sigma^2 \mathbf{I}_{LN}$, where $v \in \{1, \dots, K-1\}$ and $l \in \{1, \dots, L\}$. $\mathbf{H}_{ev}^{(l)} \in \mathbb{R}^{LN \times LN}$ represents the channel between the l th user and eavesdropper v and \mathbf{w}_{ev} corresponds to the zero-mean additive white Gaussian noise with covariance matrix $\sigma^2 \mathbf{I}_{LN}$, for $v \in \{1, \dots, K-1\}$ and $l \in \{1, \dots, L\}$. We further assume a power constraint on the transmitted signal of each user $E \left\{ \|\mathbf{V}^{(l)} \mathbf{x}^{(l)}\|_2^2 \right\} \leq P$ and $(\mathbf{V}^{(l)})^T \mathbf{V}^{(l)} = \frac{P}{N} \mathbf{I}_N$, for some $P > 0$, and all $l \in \{1, \dots, L\}$. We assume that the elements of all channel matrices are drawn i.i.d. from a continuous distribution and at each channel use all receivers and transmitters have perfect channel knowledge.

We proceed by rewriting (7) and (8) as

$$\mathbf{y} = \begin{bmatrix} \mathbf{H}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \mathbf{x} + \mathbf{w}$$

$$\text{and } \mathbf{y}_{ev} = \begin{bmatrix} \mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \mathbf{x} + \mathbf{w}_{ev}$$

and defining

$$\mathbf{H} \triangleq \begin{bmatrix} \mathbf{H}^{(1)} & \dots & \mathbf{H}^{(L)} \\ \mathbf{H}_{e1}^{(1)} & \dots & \mathbf{H}_{e1}^{(L)} \\ \vdots & \vdots & \vdots \\ \mathbf{H}_{e(K-1)}^{(1)} & \dots & \mathbf{H}_{e(K-1)}^{(L)} \end{bmatrix} \in \mathbb{R}^{KLN \times LN}, \quad (9)$$

which denotes an instance of an $(L, N)^{K-1}$ multiple-access compound wiretap channel. We further define the concatenation of all L beamforming matrices

$$\mathbf{V} \triangleq \begin{bmatrix} \mathbf{V}^{(1)} & \dots & \mathbf{V}^{(L)} \end{bmatrix} \in \mathbb{R}^{LN \times LN}. \quad (10)$$

Then, to achieve the secure sum capacity for perfect secrecy of an $(L, N)^{K-1}$ multiple-access compound wiretap channel at the high SNR regime, we have to maximize the sum S-DoF. For this case the sum S-DoF of an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , for a given set of beamforming matrices \mathbf{V} , and assuming $\mathbf{x}^{(l)}$, $l \in \{1, \dots, L\}$, is a zero-mean real Gaussian vector with covariance matrix \mathbf{I}_N , is given by

$$\eta \left((L, N)^{K-1}, \mathbf{H}, \mathbf{V} \right) \triangleq \frac{\text{rank} \left(\begin{bmatrix} \mathbf{H}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \right) - \max_{v \in \{1, \dots, K-1\}} \text{rank} \left(\begin{bmatrix} \mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \right)}{LN} \quad (11)$$

where $[a]^+ = \begin{cases} a, & a \geq 0, \\ 0, & a < 0 \end{cases}$. Hence, the set of beamforming matrices \mathbf{V} has to be designed such that the legitimate signal space spans the maximum dimensions possible and each of the

$K-1$ eavesdropper signal spaces have to collapse in as small dimensions as possible, such that the maximum dimension spanning space is minimized.

Observe that given a signal space $[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)}]$ spanning LN dimensions, the S-DoF of an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} can be maximized by solving the following optimization problem

$$\begin{aligned} & \mathcal{V} \left((L, N)^{K-1}, \mathbf{H} \right) : \\ & \min_{\mathbf{V}^{(1)}, \dots, \mathbf{V}^{(L)}} \max_{v \in \{1, \dots, K-1\}} \text{rank} \left(\begin{bmatrix} \mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \right) \\ & \text{s.t.: } \text{rank} \left(\begin{bmatrix} \mathbf{H}^{(1)} \mathbf{V}^{(1)} & \dots & \mathbf{H}^{(L)} \mathbf{V}^{(L)} \end{bmatrix} \right) = LN. \end{aligned}$$

Lemma 2: For a given $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , solving $\mathcal{V} \left((L, N)^{K-1}, \mathbf{H} \right)$ is equivalent to maximizing the total S-DoF, when the legitimate signal space spans LN dimensions.

We note that the minimum rank of an eavesdropper’s observable space cannot be less than N assuming that the beamforming matrices are full column rank due to each beamforming matrix being full rank. The following bound

$$\eta \left((L, N)^{K-1}, \mathbf{H}, \mathbf{V} \right) \leq \frac{LN - N}{LN} = \frac{L-1}{L} \quad (12)$$

always serves as an outerbound to the achievable sum S-DoF.

In the next section, we establish a connection between the S-DoF maximization and the repair overhead minimization.

IV. ESTABLISHING THE CONNECTIONS

The two models of sections II and III correspond to physically unrelated settings. In the following, we state linear algebraic analogies between the two model descriptions of the two cases followed by analogies in the objectives of each optimization problem. Eventually, the analogies aid a formal connection between the overhead minimization and the S-DoF maximization.

We begin by observing that for both overhead minimization and S-DoF maximization setups, there exist two types of algebraic spaces with respect to the respective objectives: the “useful” spaces and the “harmful” spaces. The useful spaces need always be full rank for both problems. Then, the sum of dimensions of the set of harmful spaces for the first problem, or the maximum dimension of harmful space for the second, need to be minimized respectively. Specifically, for the overhead minimization problem, the useful space when we repair node i is $[\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)}]$, while the $k-1$ interference spaces $[\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)}]$, $u \in \{1, \dots, k\} \setminus i$, consist harmful components; the larger their sum of dimensions, the larger the overhead to repair systematic node $i \in \{1, \dots, k\}$. Then, for the S-DoF maximization, the useful space is $[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)}]$, while there exist $K-1$ eavesdropper spaces $[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)}]$, $v \in \{1, \dots, K-1\}$, that potentially harm the objective; the larger the maximum of their dimensions, the lower the S-DoF.

OVERHEAD MINIMIZATION FOR REPAIR OF NODE i			S-DoF Maximization	
Spaces				
Useful data space	$\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)}$		$\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)}$	Legitimate receiver space
Interference space	$\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)}$		$\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)}$	Eavesdropper's space
Matrices				
Code matrix	$\mathbf{P}_i \mathbf{A}$		\mathbf{H}	Channel matrix
Repair strategy	\mathbf{R}_i		\mathbf{V}	Beamforming strategy
Dimensions				
# Parity nodes	$n - k$		L	# Users
# Interference spaces	$k - 1$		$K - 1$	# Wiretapped spaces
Subpacketization	β		N	# Symbols/User
Constraints				
$\text{rank} \left(\left[\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \right) = (n - k) \beta$			$\text{rank} \left(\left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)} \right] \right) = LN$	
Cost functions ^(*)				
$\sum_{u=1, u \neq i}^k \text{rank} \left(\left[\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \right)$			$\min_{v \in \{1, \dots, K-1\}} \text{rank} \left(\left[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \right] \right)$	

Fig. 2. ANALOGIES

Furthermore, we observe that each parity node $p \in \{1, \dots, n - k\}$ and each user $l \in \{1, \dots, L\}$ is associated with a repair matrix $\mathbf{R}_i^{(p)}$ and a beamforming matrix $\mathbf{V}^{(l)}$, respectively. The two matrices multiply i) one matrix ($\mathbf{A}_i^{(p)}$ or $\mathbf{H}^{(l)}$ respectively) contributing to useful space and ii) $k - 1$ or $K - 1$ matrices ($\mathbf{A}_u^{(p)}$, $u \in \{1, \dots, k\} \setminus i$, or $\mathbf{H}_{ev}^{(l)}$, $v \in \{1, \dots, K - 1\}$, respectively) contributing to harmful space. Then, given an $(n, k)_\beta$ MDS code \mathbf{A} , we need to optimize over the $n - k$ matrices $\mathbf{R}_i^{(1)}, \dots, \mathbf{R}_i^{(n-k)}$ to minimize the sum of interference space dimensions; that way the overhead to repair node i is minimized. Analogously, for a given $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , we need to optimize over L matrices $\mathbf{V}^{(1)}, \dots, \mathbf{V}^{(L)}$ so that the largest eavesdropper space is minimized; hence, the S-DoF is maximized. We will show that these analogies correspond to direct code-to-channel or channel-to-code mappings from one setting to another for a single repair when the codes considered are optimal or the channels achieve the outerbound of (12). When considering conventional MDS codes and more general multiple-access compound wiretap channels, we establish performance bounds in terms of repair overhead and achievable S-DoF. All analogies stated in this section are given in Fig. 2. (*) denotes that the analogy holds for optimal MDS codes. Any proofs to theorems and lemmas following are given in the Appendix.

A. Reductions

In the following, we formally state the connections between the repair overhead minimization for optimal MDS codes with the S-DoF maximization for channels that achieve (12). The connections are articulated through reductions with respect to \mathcal{R} and \mathcal{V} , code-to-channel and channel-to-code mappings for MDS codes and multiple-access compound wiretap channels,

and constructive examples.²

Theorem 1: Let an optimal $(n, k)_\beta$ MDS code \mathbf{A} . Then, $\mathcal{R}((n, k)_\beta, \mathbf{P}_i \mathbf{A})$ reduces to $\mathcal{V}((n - k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A})$, for all $i \in \{1, \dots, k\}$.

Corollary 1: Let an optimal $(n, k)_\beta$ MDS code \mathbf{A} , defined over \mathbb{R} . Then, \mathbf{A} maps to k , $(n - k, \beta)^{k-1}$ multiple-access compound wiretap channel instances $\mathbf{H} = \mathbf{P}_i \mathbf{A}$, $\forall i \in \{1, \dots, k\}$, where the outer bound of $\frac{n-k-1}{n-k}$ S-DoF is achievable.

Following Theorem 1, we establish a reverse reduction, that is for the S-DoF maximization for the class of multiple-access compound wiretap channels where (12) is achievable.

Theorem 2: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , where exactly $\frac{L-1}{L}$ S-DoF is achievable. Then, $\mathcal{V}((L, N)^{K-1}, \mathbf{H})$ reduces to $\mathcal{R}((L + K, K)_N, \mathbf{H})$.

Corollary 2: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , where $\frac{L-1}{L}$ S-DoF is achievable. Then, \mathbf{H} maps to an $(L + K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$, where the overhead to repair systematic node 1 is $\frac{n-1}{n-k}$.

Remark: If the elements of \mathbf{H} are drawn i.i.d. from a continuous distribution, then \mathbf{H} maps to an optimal $(L + K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$.

The two reductions provided by Theorems 1 and 2 state that if there existed a black-box that could solve $\mathcal{V}((L, N)^{K-1}, \mathbf{H})$, then this box could be used to solve $\mathcal{R}((n, k)_\beta, \mathbf{P}_i \mathbf{A})$ for optimal MDS codes. A vice versa statement holds for multiple-access compound wiretap channels where (12) is achievable. We establish that optimal MDS codes map to channels where (12) is achievable. Accordingly, channels where (12) is tight map to MDS codes where the repair of a single node can be performed with minimum overhead.

²Henceforth, we assume that an algorithm solving \mathcal{R} over a finite field \mathbb{F} can be converted to one over \mathbb{R} , for any $i \in \{1, \dots, k\}$, and an algorithm solving \mathcal{V} over \mathbb{R} can be converted to one over \mathbb{F} .

For the channel-to-code mapping any channel that satisfies the MDS property (i.e. all sub-matrices are full rank) maps to a code that is always of practical interest. In sharp contrast, the code-to-channel mapping is of practical interest only when the structure of \mathbf{A} is not artificial and can represent realistic $(n-k, \beta)^{K-1}$ multiple-access compound wiretap channel structures. The most interesting example comes for free after applying Corollary 1 on the asymptotically optimal MDS code presented in [19] and [20]. We use the code-to-channel mapping to show that the outerbound of (12) is asymptotically achievable and establish the S-DoF of the single antenna multiple-access compound wiretap channel; this is possible by mapping the repair matrices to the beamforming matrices used by the users of such system.

Example 1: In this example, we show that $\frac{L-1}{L}$ S-DoF is achievable for the single antenna, time-varying, multiple-access compound wiretap channel, with L users and $K-1$ eavesdroppers. To achieve such result, we use symbol extension and set the beamforming matrices equal to the repair matrices used for the asymptotically optimal MDS code presented in [19] and [20], that maps to the same channel structure. Most interestingly, in [19] and [20] the authors prove the asymptotical achievability of the information theoretic minimum overhead for the exact repair of departed nodes for MDS codes of any rate, for $\beta \rightarrow \infty$. Although this MDS code was presented for finite fields, through this example we show that the mapping also works over the reals. Moving to the single antenna, time-varying, L users, $K-1$ eavesdroppers, multiple-access compound wiretap channel, the received signals at the legitimate receiver and the k th eavesdropper at a single channel use are

$$y(t) = \sum_{l=1}^L h^{(l)}(t) \hat{x}^{(l)}(t) + w(t)$$

$$\text{and } y_{ev}(t) = \sum_{l=1}^L h_{ev}^{(l)}(t) \hat{x}^{(l)}(t) + w_{ev}(t),$$

respectively, where $h^{(l)}(t) \in \mathbb{R}$ represents the channel between the l th user and the legitimate receiver at time t , $h_{ev}^{(l)}(t) \in \mathbb{R}$ the channel between the l th user and v th eavesdropper, and $w(t)$ and $w_{ev}(t)$ account for zero-mean additive white Gaussian noise with variance σ^2 at the legitimate receiver and eavesdropper v , respectively, where $l \in \{1, \dots, L\}$ and $v \in \{1, \dots, K-1\}$. $\hat{x}^{(l)}(t) \in \mathbb{R}$ is the symbol that user $l \in \{1, \dots, L\}$ transmits.

Then, we employ $LN = L\Delta^{(K-1)L}$ symbol extensions such that

$$\begin{bmatrix} \hat{x}^{(l)}(1) \\ \vdots \\ \hat{x}^{(l)}(LN) \end{bmatrix} = \mathbf{V}^{(l)} \mathbf{x}^{(l)}, \mathbf{H}^{(l)} = \begin{bmatrix} h^{(l)}(1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & h^{(l)}(LN) \end{bmatrix}, \text{ and}$$

$$\mathbf{H}_{ev}^{(l)} = \begin{bmatrix} h_{ev}^{(l)}(1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & h_{ev}^{(l)}(LN) \end{bmatrix},$$

for $\Delta \in \mathbb{N}^+$, $l \in \{1, \dots, L\}$, and $v \in \{1, \dots, K-1\}$. Observe that we may perceive this symbol extended channel as an $(L, \Delta^{(K-1)L})^{K-1}$ multiple-access compound wiretap channel, where the channel matrices are diagonal. The structure of the individual channel matrices is in accordance with

the diagonal structure of the coding matrices in [19] and [20]. Specifically, every code $(n, k)_\beta$ \mathbf{A} of [19] and [20], with diagonal elements drawn from a continuous distribution, maps to an $(L, N)^{K-1}$ channel with matrices having the same diagonal structure described earlier, for $n-k = L$, $\beta = N$, and $k = K$. For our setting we set the beamforming matrices equal to the repair matrices of [19] and [20], that achieve the minimum repair overhead. Namely,

$$\hat{\mathbf{V}} = \mathbf{V}^{(l)} = \left\{ \left(\prod_{l'=1}^L \prod_{v=1}^{K-1} \left(\mathbf{H}_{ev}^{(l')} \right)^{\alpha_{l',v}} \right) \mathbf{w} : \alpha_{l',v} \in \{1, \dots, \Delta\} \right\},$$

for all $l \in \{1, \dots, L\}$, where we assume the elements of $\mathbf{w} \in \mathbb{R}^{L\Delta^{(K-1)L}}$ to be drawn i.i.d. from a continuous distribution. Hence, $\hat{\mathbf{V}}$ has $\Delta^{(K-1)L}$ linearly independent column vectors almost surely. Then, we obtain the following

$$\text{rank} \left(\left[\mathbf{H}^{(1)} \mathbf{V} \dots \mathbf{H}^{(L)} \mathbf{V} \right] \right) = L\Delta^{(K-1)L}$$

$$\text{and } \Delta^{(K-1)L} < \text{rank} \left(\left[\mathbf{H}_{ev}^{(1)} \mathbf{V} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V} \right] \right) < (\Delta+1)^{(K-1)L},$$

with probability 1, when the channel coefficients are drawn i.i.d. from a continuous distribution. For this channel we achieve the following S-DoF

$$\eta \left(\left(L, \Delta^{(K-1)L} \right)^{K-1}, \mathbf{H}, \mathbf{V} \right) = \frac{L\Delta^{(K-1)L} - (\Delta+1)^{(K-1)L}}{L\Delta^{(K-1)L}}$$

$$\xrightarrow{\Delta \rightarrow \infty} \frac{L-1}{L} \quad (13)$$

almost surely and asymptotically match the outer bound of (12) for $\Delta \rightarrow \infty$. Interestingly, this result is not a function of the number of eavesdroppers, which is in accordance to the MISO compound wiretap setup of [7]. As a sidenote, we observe that the single antenna case of our channel model can be seen as a MISO compound wiretap system where the beamforming is done independently at each antenna element over time, still yielding the same S-DoF as in [7].

We continue with another code-to-channel mapping example. This case is a straightforward extension of the $(L, 1)^1$ multiple-access wiretap channel of [8], for users wishing to transmit more than 1 symbols.

Example 2: Let an $(n, 2)_\beta$ MDS code \mathbf{A} , where each element of \mathbf{A} is drawn i.i.d. from a continuous distribution. Then, an optimal set of repair vectors for the repair of node i are $\mathbf{R}_i = \left[\left(\mathbf{A}_u^{(1)} \right)^{-1} \mathbf{W} \dots \left(\mathbf{A}_u^{(n-k)} \right)^{-1} \mathbf{W} \right]$, where $\mathbf{W} \in \mathbb{R}^{(n-k)\beta \times \beta}$ is also drawn i.i.d. from a continuous distribution and $(i, u) \in \{(1, 2), (2, 1)\}$. These repair matrices yield an interference space of dimension β . Namely, for the repair of systematic node $i \in \{1, 2\}$ we have

$$\text{rank} \left(\begin{bmatrix} \left(\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \right)^T \\ \vdots \\ \left(\mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \right)^T \end{bmatrix} \right) = \text{rank} \left(\begin{bmatrix} (\mathbf{W})^T \\ \vdots \\ (\mathbf{W})^T \end{bmatrix} \right) = \beta,$$

for $(i, u) \in \{(1, 2), (2, 1)\}$, while obeying the full rank constraint with probability 1. Since we posed no constraints on the elements of \mathbf{A} , the code \mathbf{A} maps to an $(n-k, \beta)^1$ multiple-access wiretap channel $\mathbf{H} = \mathbf{A}$. To achieve (12) for

\mathbf{H} , we use as beamforming matrices the repair matrices $\hat{\mathbf{R}}_1$, i.e. $\mathbf{V}^{(l)} = (\mathbf{H}_{e1}^{(l)})^{-1} \mathbf{W}$. Then,

$$\text{rank} \left(\begin{bmatrix} (\mathbf{H}_{e1}^{(1)} \mathbf{V}^{(1)})^T \\ \vdots \\ (\mathbf{H}_{e1}^{(n-k)} \mathbf{V}^{(n-k)})^T \end{bmatrix} \right) = \text{rank} \left(\begin{bmatrix} (\mathbf{W})^T \\ \vdots \\ (\mathbf{W})^T \end{bmatrix} \right) = \beta,$$

and $\text{rank}([\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(n-k)} \mathbf{V}^{(n-k)}]) = (n-k)\beta$, almost surely. Thus, $\frac{n-k-1}{n-k}$ S-DoF is almost surely achievable for all, but a measure zero set of, $(n-k, \beta)^1$ multiple-access wiretap channels. Since $n-k, \beta \in \mathbb{N}^+$, this result can be equivalently stated for $(L, N)^1$ channels, for any $L, N \in \mathbb{N}^+$.

Next, we exhibit a channel-to-code mapping, where we rederive the optimal $(n, 2)$ MDS code of [13] using the channel matrices of [8].

Example 3: Let an $(L, 1)^1$ multiple-access compound wiretap channel \mathbf{H} . Then, by setting $\mathbf{v}^{(l)} = (\mathbf{H}_{e1}^{(l)})^{-1} \mathbf{e}_1$, for $l \in \{1, \dots, L\}$, such that $\mathbf{H}_{e1}^{(l)} \mathbf{v}^{(l)} = \mathbf{e}_1$, we obtain $[\mathbf{H}_{e1}^{(1)} \mathbf{v}^{(1)} \dots \mathbf{H}_{e1}^{(L)} \mathbf{v}^{(L)}] = [\mathbf{e}_1 \dots \mathbf{e}_1]$, and achieve (12), almost surely. Any such randomly drawn $(L, 1)^1$ channel maps to an optimal $(L+2, 2)_1$ MDS code $\mathbf{A} = \mathbf{H}$, or equivalently, to an optimal $(n, 2)_1$ MDS code \mathbf{A} . For such a code we set $\mathbf{R}_1 = [(\mathbf{A}_2^{(1)})^{-1} \mathbf{e}_1 \dots (\mathbf{A}_2^{(L)})^{-1} \mathbf{e}_1]$ and $\mathbf{R}_2 = [(\mathbf{A}_1^{(1)})^{-1} \mathbf{e}_1 \dots (\mathbf{A}_1^{(L)})^{-1} \mathbf{e}_1]$. Observe that these repair matrices yield an interference space of dimension $\beta = 1$ for the repair of systematic node $i \in \{1, 2\}$, that

$$\text{is rank} \left(\begin{bmatrix} (\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)})^T \\ \vdots \\ (\mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)})^T \end{bmatrix} \right) = \text{rank} \left(\begin{bmatrix} (\mathbf{e}_1)^T \\ \vdots \\ (\mathbf{e}_1)^T \end{bmatrix} \right) = 1,$$

achieving the information theoretic minimum repair overhead $\frac{L+1}{L}$.

B. General Performance Bounds

Here, we extend the results to more general MDS codes and channels. Even when considering conventional MDS codes, or multiple-access compound wiretap channels where (12) is not achievable, connections still exist; this time, in the form of achievable upper and lower bounds with respect to repair overhead and S-DoF, respectively. We derive such bounds in the following lemmas. The main point is that a code requiring a certain overhead for the repair problem can still map to a channel where some S-DoF can be achieved and vice versa. As a sidenote, performance bounds presented in this section are mainly due to the fact that $\frac{\|\mathbf{s}\|_1}{T} \leq \|\mathbf{s}\|_\infty \leq \|\mathbf{s}\|_1 \leq T\|\mathbf{s}\|_\infty$, for any $\mathbf{s} \in \mathbb{R}^T$, which we apply to the optimization objective to derive the following.

Lemma 3: Let an $(n, k)_\beta$ MDS code \mathbf{A} over \mathbb{R} and δ_i be the overhead required to repair systematic node $i \in \{1, \dots, k\}$. Then, \mathbf{A} maps to an $(n-k, \beta)^{k-1}$ multiple-access compound wiretap channel $\mathbf{H} = \mathbf{P}_i \mathbf{A}$, where at least $[2 - \delta_i]^+$ and at most $\frac{k-\delta_i}{k-1}$ S-DoF is achievable.

Lemma 4: Let an $(n, k)_\beta$ MDS code \mathbf{A} over \mathbb{R} and some set of repair matrices \mathbf{R}_i , $i \in \{1, \dots, k\}$. Then, \mathbf{A} maps to an $(n-k, \beta)^{k-1}$ multiple-access compound wiretap channel $\mathbf{H} = \mathbf{P}_i \mathbf{A}$, where $\eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i)$ S-DoF is achievable for $\mathbf{V} = \mathbf{R}_i$.

In the next example, we consider a code-to-channel mapping according to Lemma (4) and study the bounds derived by Lemma (3).

Example 4: Let an $(n, k)_\beta$ MDS code \mathbf{A} , where for the repair of node $i \in \{1, \dots, k\}$ overhead δ_i is required when using \mathbf{R}_i . Then, \mathbf{A} maps to an $(n-k, \beta)^{k-1}$ channel $\mathbf{H} = \mathbf{P}_i \mathbf{A}$, $i \in \{1, \dots, k\}$. For this channel we set $\mathbf{V} = \mathbf{R}_i$ and obtain

$$\begin{aligned} \eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) &= \eta((n-k, \beta)^{k-1}, \mathbf{H}, \mathbf{V}) \\ &\geq \left\lceil \frac{(n-k)\beta - \sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(n-k)\beta} \right\rceil^+ \\ &= [2 - \delta_i]^+ = \begin{cases} \left\lceil \frac{n-k-(k-1)}{n-k} \right\rceil^+, & \delta_i = \frac{n-1}{n-k} \\ [2-k]^+, & \delta_i = k \end{cases} \end{aligned} \quad (14)$$

and

$$\begin{aligned} \eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) &= \eta((n-k, \beta)^{k-1}, \mathbf{H}, \mathbf{V}) \\ &\leq \frac{(n-k)(k-1)\beta - \sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(k-1)(n-k)\beta} \\ &= \frac{(n-k)k\beta}{(k-1)(n-k)\beta} - \frac{\delta_i}{k-1} \\ &= \frac{k-\delta_i}{k-1} = \begin{cases} 1 - \frac{k+1}{(k-1)(n-k)}, & \delta_i = \frac{n-1}{n-k} \\ 0, & \delta_i = k \end{cases} \end{aligned} \quad (15)$$

For $k = 2$, (14) is tight for $\delta_i = \frac{n-1}{n-2}$. For any $k > 1$ and $\delta_i = k$, (15) is always tight. Here, we considered only the two extreme values of δ_i .

We continue with performance bounds for channel-to-code mappings, for channels that do not necessarily achieve (12).

Lemma 5: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , where η S-DoF is achievable. Then, \mathbf{H} maps to an $(L+K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$ over \mathbb{R} and the overhead to repair node 1 is at most $1 + (K-1)(1-\eta)$ and at least $2 - \eta$.

Lemma 6: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} and a set of beamforming matrices \mathbf{V} . Then, \mathbf{H} maps to an $(L+K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$ over \mathbb{R} , where overhead $\delta((L+K, K)_N, \mathbf{H}, \mathbf{V})$ to repair node 1 is achievable for $\mathbf{R}_1 = \hat{\mathbf{V}}$.

We consider a code-to-channel mapping according to Lemma (6) and study the bounds derived by Lemma (5).

Example 5: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , where η S-DoF is achievable using \mathbf{V} . Then, \mathbf{H} maps to an $(L+K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$. For this code we set $\mathbf{R}_1 = \mathbf{V}$ and obtain

$$\begin{aligned} \delta((L+K, K)_N, \mathbf{H}, \mathbf{V}) &= \delta((L+K, K)_N, \mathbf{A}, \mathbf{R}_1) \\ &\leq \frac{LN + (K-1) \max_{u \in \{2, \dots, K\}} \text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_1^{(n-k)}])}{LN} \\ &= 1 + (K-1)(1-\eta) = \begin{cases} \frac{L+K-1}{K}, & \eta = \frac{L-1}{L} \\ K, & \eta = 0 \end{cases} \end{aligned} \quad (16)$$

and

$$\begin{aligned} \delta((L+K, K)_N, \mathbf{H}, \mathbf{V}) &= \delta((L+K, K)_N, \mathbf{A}, \mathbf{R}_1) \\ &\geq \frac{LN + \max_{u \in \{2, \dots, K\}} \text{rank} \left(\left[\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_1^{(n-k)} \right] \right)}{LN} \\ &= 2 - \eta = \begin{cases} 1 + \frac{1}{L}, & \eta = \frac{L-1}{L} \\ 2, & \eta = 0 \end{cases}. \end{aligned} \quad (17)$$

Observe that (16) is tight for both cases and all any code considered, but (17) not. Again, we considered the two extreme values of η .

We need to note that by the previous lemmas, it is implicit that having a black-box solving either \mathcal{R} or \mathcal{V} is useful for both the repair minimization and S-DoF maximization problem, since any solution to one problem plugs in as a solution to the corresponding mapped one in the analogous setting.

To conclude, in this section we established connections between the repair overhead minimization of MDS codes and the S-DoF maximization of multiple-access compound wiretap channels.

V. CONCLUSIONS

In this work we showed that the repair overhead minimization for optimal MDS codes reduces to the S-DoF maximization in a multiple-access compound wiretap channel. The reverse holds for multiple-access compound wiretap channels where (12) is tight. The framework for the reductions was established by restating the two problems as rank constrained sum rank and max rank minimizations, respectively. Through this framework we established code-to-channel and channel-to-code mappings. Using such a mapping, we determined the maximum S-DoF in the single antenna, multiple-access compound wiretap channel. We also extended our results to conventional MDS codes and more general channels.

APPENDIX

Proof of (11): Let

$$\begin{aligned} \mathbf{S} &\triangleq \frac{1}{\sqrt{P}} \left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)} \right] \in \mathbb{R}^{LN \times LN}, \\ \mathbf{S}_{ev} &\triangleq \frac{1}{\sqrt{P}} \left[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \right] \in \mathbb{R}^{LN \times LN} \end{aligned}$$

for all $v \in \{1, \dots, K-1\}$. Then,

$$\begin{aligned} &L \cdot N \cdot \eta \left((L, N)^{K-1}, \mathbf{H}, \mathbf{V} \right) \\ &= \lim_{P \rightarrow \infty} \frac{\frac{1}{2} \log \det \left(\mathbf{I}_{M_t} + \frac{1}{\sigma^2} \sum_{l=1}^L \mathbf{H}^{(l)} \mathbf{V}^{(l)} (\mathbf{H}^{(l)})^T (\mathbf{V}^{(l)})^T \right)}{\frac{1}{2} \log \left(\frac{P}{\sigma^2} \right)} \\ &= \lim_{P \rightarrow \infty} \frac{\frac{1}{2} \log \det \left(\frac{P}{\sigma^2} \mathbf{S} \mathbf{S}^T \right) - \max_{v \in \{1, \dots, K-1\}} \frac{1}{2} \log \det \left(\frac{P}{\sigma^2} \mathbf{S}_{ev} \mathbf{S}_{ev}^T \right)}{\frac{1}{2} \log \left(\frac{P}{\sigma^2} \right)} \\ &= \lim_{P \rightarrow \infty} \frac{\sum_{i=1}^{\text{rank}(\mathbf{S})} \frac{1}{2} \log \left(\frac{P}{\sigma^2} \sigma_i^S \right) - \max_{v \in \{1, \dots, K-1\}} \sum_{i=1}^{\text{rank}(\mathbf{S}_{ev})} \frac{1}{2} \log \left(\frac{P}{\sigma^2} \sigma_i^v \right)}{\frac{1}{2} \log \left(\frac{P}{\sigma^2} \right)} \\ &= \lim_{P \rightarrow \infty} \frac{\text{rank}(\mathbf{S}) \frac{1}{2} \log \left(\frac{P}{\sigma^2} \right) - \max_{v \in \{1, \dots, K-1\}} \text{rank}(\mathbf{S}_{ev}) \frac{1}{2} \log \left(\frac{P}{\sigma^2} \right)}{\frac{1}{2} \log \left(\frac{P}{\sigma^2} \right)} \\ &= \text{rank} \left(\left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)} \right] \right) - \max_{v \in \{1, \dots, K-1\}} \text{rank} \left(\left[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)} \right] \right). \end{aligned}$$

The previous example is possible when the maximum singular values of the channel matrices are not scaling with the power P . Namely, for the i th largest singular of matrix \mathbf{S} , σ_i we obtain

$$\begin{aligned} \sigma_i &\triangleq \frac{1}{P} \max_{\|\mathbf{x}\|_2=1} \left\| \left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)} \right] \mathbf{x} \right\|_2^2 \\ &= \frac{1}{P} \max_{\|\mathbf{x}\|_2=1} \left\| \sum_{l=1}^L \mathbf{H}^{(l)} \mathbf{V}^{(l)} \mathbf{x}^{(l)} \right\|_2^2 \\ &\leq \frac{1}{P} \sum_{l=1}^L \max_{\|\mathbf{V}^{(l)} \mathbf{x}^{(l)}\|_2 \leq \sqrt{P}} \left\| \mathbf{H}^{(l)} \mathbf{x}_l \right\|_2^2 \leq \frac{1}{P} \sum_{l=1}^L P \max_{\|\mathbf{x}_l\|_2=1} \left\| \mathbf{H}^{(l)} \mathbf{x}_l \right\|_2^2 \\ &= L \max_{i \in \{1, \dots, LN\}, l \in \{1, \dots, L\}} \sigma_i \left(\mathbf{H}^{(l)} \right) \end{aligned}$$

for $\mathbf{x} = \left[(\mathbf{x}^{(1)})^T \dots (\mathbf{x}^{(L)})^T \right]^T$, $\mathbf{x}_l \in \mathbb{R}^{LN \times 1}$, for $l \in \{1, \dots, L\}$. In the same fashion, we have for the i th largest singular value of matrix \mathbf{S}_{ev} is upper bounded. Hence, the singular values are not scaling with P as long as the largest singular values of the channels are not scaling with P . \square

Proof of Theorem 1: Let an optimal $(n, k)_\beta$ MDS code \mathbf{A} and a systematic node $i \in \{1, \dots, k\}$ fail. Then, setting $L = n - k$, $N = \beta$, $K = k$, and $\mathbf{H} = \mathbf{P}_i \mathbf{A}$, accounts for constructing an $(n - k, \beta)^{k-1}$ multiple-access compound wiretap channel instance \mathbf{H} . Then, the following mappings hold

$$\begin{aligned} \left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(n-k)} \mathbf{V}^{(n-k)} \right] &= \left[\mathbf{A}_i^{(1)} \mathbf{V}^{(1)} \dots \mathbf{A}_i^{(n-k)} \mathbf{V}^{(n-k)} \right] \\ &= \left[\mathbf{A}_i^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_i^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \end{aligned}$$

and

$$\begin{aligned} \left[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(n-k)} \mathbf{V}^{(n-k)} \right] &= \left[\mathbf{A}_u^{(1)} \mathbf{V}^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{V}^{(n-k)} \right] \\ &= \left[\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \end{aligned}$$

for any $\mathbf{V} = \mathbf{R}_i$ and $v = \begin{cases} u, & u \in \{1, \dots, i-1\}, \\ u-1, & u \in \{i+1, \dots, k\}. \end{cases}$ Hence, the full rank constraint of $\mathcal{R}((n, k)_\beta, \mathbf{P}_i \mathbf{A})$ is equivalent to the full rank constraint of $\mathcal{V}((n - k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A})$. The objectives are also equivalent since the sum of ranks and the max-rank of interference spaces are optimization equivalent cost functions

$$\begin{aligned} &\min_{\mathbf{R}_i} \sum_{u=1, u \neq i}^k \text{rank} \left(\left[\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \right) \\ &= (k-1) \min_{\mathbf{R}_i} \max_{u \in \{1, \dots, k\} \setminus i} \text{rank} \left(\left[\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)} \right] \right) \\ &= (k-1) \min_{\mathbf{V}} \max_{v \in \{1, \dots, k-1\}} \text{rank} \left(\left[\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(n-k)} \mathbf{V}^{(n-k)} \right] \right) \\ &= (k-1)\beta. \end{aligned}$$

for optimal MDS codes. \square

Proof of Theorem 2: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} , where $\frac{L-1}{L}$ S-DoF is achievable. Then, setting $n = L + K$, $K = k$, $\beta = N$, and $\mathbf{A} = \mathbf{H}$, accounts for constructing an $(L + K, K)_N$ MDS code \mathbf{A} . Then, the following mappings hold

$$\begin{aligned} \left[\mathbf{A}_1^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_1^{(L)} \mathbf{R}_1^{(L)} \right] &= \left[\mathbf{H}^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{H}^{(L)} \mathbf{R}_1^{(L)} \right] \\ &= \left[\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)} \right] \end{aligned}$$

and

$$\begin{aligned} [\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(L)} \mathbf{R}_i^{(n-k)}] &= [\mathbf{H}_{ev}^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{R}_1^{(n-k)}] \\ &= [\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(L)}] \end{aligned}$$

for any $\mathbf{V} = \mathbf{R}_i$ and $v = u - 1$. The full rank constraint of $\mathcal{V}((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A})$ is equivalent to the full rank constraint of $\mathcal{R}((n, k)_\beta, \mathbf{A})$. The objectives are also equivalent since the $K-1$ times the maximum rank equals the minimum sum of eavesdropper's space ranks and we obtain equivalent cost functions

$$\begin{aligned} (K-1) \min_{\mathbf{V}} \max_{v \in \{1, \dots, K-1\}} \text{rank} \left([\mathbf{H}_{ev}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_{ev}^{(L)} \mathbf{V}^{(n-k)}] \right) \\ = (K-1) \min_{\mathbf{R}_1} \max_{u \in \{2, \dots, k\}} \text{rank} \left([\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(L)} \mathbf{R}_1^{(n-k)}] \right) \\ = \min_{\mathbf{R}_1} \sum_{u=2}^k \text{rank} \left([\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(L)} \mathbf{R}_1^{(n-k)}] \right) \\ = (k-1)\beta. \end{aligned}$$

for channels with that can achieve $\frac{L-1}{L}$ total S-DoF. This concludes the proof. \square

Proof of lemma 3: Let an $(n, k)_\beta$ MDS code \mathbf{A} over \mathbb{R} with minimum overhead to repair systematic node i equal to δ_i achieved by \mathbf{R}_i . Then, the maximum S-DoF of the $(n-k, \beta)^{k-1}$ channel $\mathbf{H} = \mathbf{P}_i \mathbf{A}$ is upper bounded by

$$\begin{aligned} \eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) &= \eta((n-k, \beta)^{k-1}, \mathbf{H}, \mathbf{V}) \\ &= \frac{(n-k)\beta - \max_{v \in \{1, \dots, K-1\}} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(n-k)\beta} \\ &\geq \left[\frac{(n-k)\beta - \sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(n-k)\beta} \right]^+ \\ &= [2 - \delta_i]^+ \end{aligned}$$

and lower bounded by

$$\begin{aligned} \eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) &= \eta((n-k, \beta)^{k-1}, \mathbf{H}, \mathbf{V}) \\ &= \frac{(n-k)\beta - \max_{v \in \{1, \dots, K-1\}} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(n-k)\beta} \\ &\leq \frac{(n-k)(k-1)\beta - \sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(n-k)} \mathbf{V}^{(n-k)}])}{(k-1)(n-k)\beta} \\ &= \frac{(n-k)k\beta}{(k-1)(n-k)\beta} - \frac{\delta_i}{k-1}. \end{aligned}$$

for $\mathbf{V} = \mathbf{R}_i$, $i \in \{1, \dots, k\}$. This concludes the proof. \square

Proof of lemma 4: Let an $(n, k)_\beta$ MDS code \mathbf{A} over \mathbb{R} , and the set \mathbf{R}_i of repair matrices for the repair of systematic node $i \in \{1, \dots, k\}$, satisfying the constraint of $\mathcal{R}_i((n, k)_\beta, \mathbf{P}_i \mathbf{A})$. We define the $(n-k, \beta)^{k-1}$ channel instance $\mathbf{H} = \mathbf{P}_i \mathbf{A}$. Then,

by setting $\mathbf{V} = \mathbf{R}_i$ we achieve the following S-DoF for \mathbf{H}

$$\begin{aligned} &\frac{\text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)}])}{(n-k)\beta} \\ &- \frac{\max_{u \in \{1, \dots, k\} \setminus i} \text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)}])}{(n-k)\beta} \\ &= \frac{(n-k)\beta - \max_{u \in \{1, \dots, k\} \setminus i} \text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_i^{(1)} \dots \mathbf{A}_u^{(n-k)} \mathbf{R}_i^{(n-k)}])}{(n-k)\beta} \\ &= \eta((n-k, \beta)^{k-1}, \mathbf{P}_i \mathbf{A}, \mathbf{R}_i) = \eta((n-k, \beta)^{k-1}, \mathbf{H}, \mathbf{V}). \end{aligned}$$

This concludes the proof. \square

Proof of lemma 5: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} where η S-DoF is achievable by \mathbf{V} . Then, let us define the $(L+K, K)_N$ MDS code $\mathbf{A} = \mathbf{H}$. For this code we have

$$\begin{aligned} \delta((L+K, K)_N, \mathbf{H}, \mathbf{V}) &= \delta((L+K, K)_N, \mathbf{A}, \mathbf{R}_1) \\ &\leq \frac{LN + (K-1) \max_{u \in \{2, \dots, K\}} \text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(L)} \mathbf{R}_1^{(L)}])}{LN} \\ &= 1 + (K-1)(1-\eta) \end{aligned}$$

and

$$\begin{aligned} \delta((L+K, K)_N, \mathbf{H}, \mathbf{V}) &= \delta((L+K, K)_N, \mathbf{A}, \mathbf{R}_1) \\ &\geq \frac{LN + \max_{u \in \{2, \dots, K\}} \text{rank}([\mathbf{A}_u^{(1)} \mathbf{R}_1^{(1)} \dots \mathbf{A}_u^{(L)} \mathbf{R}_1^{(L)}])}{LN} = 2 - \eta. \end{aligned}$$

for $\mathbf{R}_1 = \mathbf{V}$. This concludes the proof. \square

Proof of lemma 6: Let an $(L, N)^{K-1}$ multiple-access compound wiretap channel \mathbf{H} and the set \mathbf{V} of beamforming matrices, satisfying the constraint of $\mathcal{V}_i((L, N)^{K-1}, \mathbf{H})$. We define the $(L+K, K)_N$ MDS code instance $\mathbf{A} = \mathbf{H}$. Then, by setting $\mathbf{R}_1 = \mathbf{V}$ we achieve the following overhead for the repair of node 1

$$\begin{aligned} &\frac{\text{rank}([\mathbf{H}^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}^{(L)} \mathbf{V}^{(L)}])}{LN} \\ &+ \frac{\sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(L)} \mathbf{V}_i^{(L)}])}{LN} \\ &= \frac{LN + \sum_{v=1}^{K-1} \text{rank}([\mathbf{H}_v^{(1)} \mathbf{V}^{(1)} \dots \mathbf{H}_v^{(L)} \mathbf{V}^{(L)}])}{LN} \\ &= \delta((n, k)_\beta, \mathbf{H}, \mathbf{V}). \end{aligned}$$

This concludes the proof. \square

REFERENCES

- [1] M. Maddah-Ali, A. Motahari, and A. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," in *IEEE Trans. on Inform. Theory*, pp. 3457–3470, Aug. 2008.
- [2] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K -user interference channel," in *IEEE Trans. on Inform. Theory*, vol. 54, pp. 3425–3441, Aug. 2008.
- [3] S. Jafar and S. Shamai, "Degrees of freedom region for the mimo X channel," in *IEEE Trans. on Inform. Theory*, vol. 54, Jan. 2008.

- [4] T. Gou and S. Jafar, "Degrees of freedom of the K user mimo interference channel," in *42nd Asilomar Conf. on Signals, Systems and Computers 2008*, (Pacific Grove, CA, USA), Oct. 2008.
- [5] C. Suh and D. Tse, "Interference alignment for cellular networks," in *Proceedings of 40th Annual Allerton Conf. on Commun., Control, and Computing 2008*, (Urbana-Champaign, IL, USA), Sep. 2008.
- [6] O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the k -user gaussian interference channel," May 2008. Available online at arXiv:0805.1340v1 [cs.IT].
- [7] A. Khisti, "Interference alignment for the multi-antenna compound wiretap channel," Mar. 2010. Available online at arXiv:1002.4548v2 [cs.IT].
- [8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," Mar. 2010. Available online at arXiv:1003.0729v1 [cs.IT].
- [9] M. Kobayashi, P. Piantanida, S. Yang, and S. Shamai, "On the secrecy degree of freedom of the multi-antenna block fading wiretap channels," May 2010. Available online at arXiv:1001.2410v2 [cs.IT].
- [10] X. He and A. Yener, "The gaussian many-to-1 interference channel with confidential messages," May 2010. Available online at arXiv:1005.0624v1 [cs.IT].
- [11] R. Bassily and S. Ulukus, "Ergodic secret alignment for the fading multiple access wiretap channel," in *Proc. ICC 2010*, (Cape Town, South Africa), May 2010.
- [12] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," in *IEEE Transactions on Information Theory* (to appear).
- [13] Y. Wu and A. G. Dimakis, "Reducing repair traffic for erasure coding-based storage via interference alignment," in *IEEE Int. Symp. on Information Theory (ISIT)*, (Seoul, Korea), July 2009.
- [14] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Available online at arXiv:1004.4438v1 [cs.IT].
- [15] D. Cullina, A. G. Dimakis, and T. Ho, "Searching for minimum storage regenerating codes," Oct. 2009. Available online at arXiv:0910.2245v1 [cs.IT].
- [16] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, "Explicit construction of optimal exact regenerating codes for distributed storage," Oct. 2009. Available online at arXiv:0906.4913v2 [cs.IT].
- [17] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, "Interference alignment as a tool in network coding as applied to distributed storage," in *Proc. National Conf. on Commun.*, (Chennai, India), Jan. 2010.
- [18] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, "The miser code: an mds distributed storage code that minimizes repair bandwidth for systematic nodes through interference alignment," May 2010. Available online at arXiv:0908.2984v2 [cs.IT].
- [19] V. R. Cadambe, S. A. Jafar, and H. Maleki, "Distributed data storage with minimum storage regenerating codes - exact and functional repair are asymptotically equally efficient," Apr. 2010. Available online at arXiv:1004.4299v1 [cs.IT].
- [20] C. Suh and K. Ramchandran, "On the existence of optimal exact-repair mds codes for distributed storage," Apr. 2010. Available online at arXiv:1004.4663v1 [cs.IT].
- [21] D. Papailiopoulos and A. Dimakis, "Interference alignment as a rank constrained rank minimization," in *IEEE GLOBECOM 2010*, (Miami, FL, USA).