Ong, Lawrence "Capacity results for the multi-way relay channel with common messages" Originally published in the Proceedings of the 2015 IEEE International Symposium on Information Theory (Hong Kong 14-19 June, 2015) p. 1886-1890 (2015)

Available from: http://dx.doi.org/10.1109/ISIT.2015.7282783

Capacity Results for the Multi-Way Relay Channel with Common Messages

Lawrence Ong
School of Electrical Engineering and Computer Science, The University of Newcastle, Australia

***Abstract*—We consider the multi-way relay channel with common messages and full data exchange, where multiple users exchange correlated messages through a relay. We propose an optimal coding scheme and show that it achieves (i) the capacity region if the uplink is a finite-field channel and the downlink is any arbitrary channel and (ii) the full degrees-of-freedom region if the channel is a multiple-input multiple-output (MIMO) additive white Gaussian noise (AWGN) channel.**

***Index Terms*—Multi-way relay channel, capacity, degrees of freedom, MIMO, AWGN**

I. Introduction

Relaying is an important aspect in wireless communications. Acting as repeaters, they boost exponentially decaying signal strength (as the distance increases); acting as base stations, they coordinate transmissions among multiple devices. In this paper, we study the *multi-way relay channel* where multiple devices (referred to as the *users*) communicate through a relay. This wireless network structure is commonly deployed today in, e.g., satellite networks and cellular mobile networks.

The capacity of the multi-way relay channel remains unknown to date, except for some special cases [1], [2]. A main challenge is to determine how the relay should facilitate data exchange among the users—what to decode and what to relay.

In this paper, we focus on the multi-way relay channel with *correlated messages* (where the users may have parts of their messages in common) and *full data exchange* (where each user sends its message to all other users). We derive

1) the capacity region if the uplink (i.e., the link from the users to the relay) is a finite-field channel, and
2) the *degrees-of-freedom* (DOF) region (i.e., asymptotic capacity in the high signal-to-noise regime) if the channel is a multiple-input multiple-output (MIMO) additive white Gaussian noise (AWGN) channel.

To this end, we design an optimal function (of the messages) that the relay should decode, by carefully scheduling when the users should transmit which part of their messages.

A. Related Work and Our Contributions

Consider the multi-way relay channel depicted in Fig. 1 with full data exchange. When the users' messages are independent, the capacity region has been found if the channel is any finite-field channel [1], or the uplink is any deterministic channel [2]. The equal-rate capacity (all users transmitting at the same rate) has been found for the symmetrical AWGN channel [3].

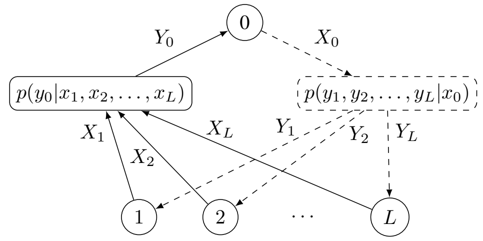
Y_0
0
X_0
$p(y_0|x_1, x_2, \ldots, x_L)$
$p(y_1, y_2, \ldots, y_L|x_0)$
X_1
X_2
X_L
Y_1
Y_2
Y_L
1
2
$\cdots$
L

Fig. 1. The multi-way relay channel, where users, nodes $1, 2, \ldots, L$, exchange correlated messages with the help of a relay, node 0, through an uplink (drawn with solid lines) and a downlink (drawn with dashed lines)

When the users' messages are correlated, the problem becomes significantly more difficult. Here, we consider a special and useful correlation structure where the messages comprise independent sub-messages, and each sub-message is known to one or more users. We refer to this message structure as common messages (see Han [4] and also common information in the sense of Gács and Körner [5]).

For the *three-user* finite-field channel with common messages, Ong et al. [6] designed an optimal coding function[1] and showed that the coding function achieves the capacity region. This function is, however, specific to only three users. A year later, Ong et al. [7] designed an optimal coding function for any number of users, but the common messages are restricted to only pair-wise, meaning that any sub-message can be known to at most two users.

In this paper, we extend the coding function for pair-wise common messages and introduce a crucial *new step*, and show that our new scheme can achieve the capacity region of the finite-field channel for all common messages (not restricted to pair-wise) for any number of users.

The finite-field channel (see equation (1)) shares many similarities with the more-widely-used AWGN model (e.g., both are linear). We have shown that insights from the finite-field channel are useful for the AWGN channel [3]. In this paper, we further show the utility of analyzing the finite-field channel: by showing that the optimal coding function designed for the finite-field channel is also asymptotically optimal in the MIMO AWGN channel at high transmitted power, i.e., it achieves the full degrees-of-freedom (DOF) region.

DOF studies the asymptotic capacity of communication networks as the transmitted power grows to infinity. It provides insights to optimal allocation of resources—in the time, frequency, and spatial dimensions—in the network. The DOF

Lawrence Ong is the recipient of an Australian Research Council Future Fellowship (FT140100219).

[1] Function of messages that the relay should decode on the uplink

region of the MIMO AWGN multi-way relay channel is also an open problem to date. Current studies on the DOF of the MIMO AWGN multi-way relay channel focus on independent messages and private message exchange[2] (see, e.g., Lee et al. [8], Tian and Yener [9], Chaaban et al. [10], and the references therein). The techniques used therein first orthogonalize the MIMO uplink, and let *at most two users* transmit their messages on each orthogonal sub-link. The relay then decodes a function of the transmitted messages (at most two) on each sub-link.

We observe that a key difference between the optimal coding function for the multi-way relay channel with independent messages and that with common messages is that the relay decodes functions of at most two messages in the former, but of more than two messages in the latter.

II. Channel Model

The multi-way relay channel, depicted in Fig. 1 consists of an uplink conditional probability mass function (pmf) $p_{Y_0|X_1,X_2,\dots,X_L}(y_0|x_1,x_2,\dots,x_L)$ and a downlink conditional pmf $p_{Y_1,Y_2,\dots,Y_L|X_0}(y_1,y_2,\dots,y_L|x_0)$, where $X_i \in \mathcal{X}_i$ and $Y_i \in \mathcal{Y}_i$ are input and output of node i respectively.

Define the following independent messages:[3] $\{W_{\mathtt{I}} : \mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L])\}$, where $\mathcal{P}_{\leq L-1}([1:L])$ is the set of all subsets of $[1:L]$ with cardinality between one and $L-1$ (inclusive). For example, $\mathcal{P}_{\leq 2}([1:3]) = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\}$. Here, we have used the notation $[a:b] \triangleq \{a,a+1,\dots,b\}$.

Messages $\{W_{\mathtt{I}} : a \in \mathtt{I}\}$ are given to node a a priori. Denote the set of indices of all messages that node a knows by

$$\mathcal{K}_a \triangleq \{\mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L]) : a \in \mathtt{I}\}, \tag{1}$$

and that for all messages that node a wants by

$$\mathcal{W}_a \triangleq \{\mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L]) : a \notin \mathtt{I}\}. \tag{2}$$

We have $\mathcal{W}_a = \mathcal{P}_{\leq L-1}([1:L]) \setminus \mathcal{K}_a$, i.e., each user wants all messages that it does not know.

Consider n uses of the channel (uplink and downlink simultaneously). Let $W_{\mathtt{I}}$ be randomly distributed on $[1:2^{nr_{\mathtt{I}}}]$, for some integer $2^{nr_{\mathtt{I}}}$. Here, $r_{\mathtt{I}}$ is the transmission rate of $W_{\mathtt{I}}$ in bits per channel use. Let the channel input and output of node a on the t-th channel use be $X_a[t]$ and $Y_a[t]$ respectively. A block code consists of (i) encoding functions for each node $a \in [0:L]$: $X_a[t] = f_{a,t}(W_{\mathcal{K}_a}, Y_a[1],\dots,Y_a[t-1])$, for $t \in [1:n]$, where $W_{\mathcal{S}} \triangleq (W_a : a \in \mathcal{S})$, $\mathcal{K}_0 = \emptyset$; (ii) a decoding function for each user $a \in [1:L]$: $\widehat{W}_{\mathcal{W}_a} = g_a(W_{\mathcal{K}_a}, Y_a[1],\dots,Y_a[n])$, where $\widehat{W}_{\mathcal{W}_a}$ is user a's estimate of $W_{\mathcal{W}_a}$.

The rate tuple $\boldsymbol{r} = (r_{\mathtt{I}} : \mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L])$ is said to be achievable if, for any $\epsilon > 0$, we can find a sufficiently large n and some block code $\{f_{a,t}, g_a\}$ such that the probability that some user(s) wrongly decodes some message(s) is smaller than ϵ. The capacity is the closure of the set of all achievable $\boldsymbol{r}$.

III. Results

We state our capacity results in this section, and present the proofs in subsequent sections. Our results are expressed using the following notation. The sum rate of all messages that node a needs to decode is

$$r_a^{\Sigma} \triangleq \sum_{\mathtt{I} \in \mathcal{W}_a} r_{\mathtt{I}}, \tag{3}$$

and the largest sum rate (among all users) to be decoded is

$$r_{\max}^{\Sigma} \triangleq \max_{a \in [1:L]} r_a^{\Sigma}. \tag{4}$$

A. Finite-Field Uplink and Arbitrary Downlink

For a finite-field uplink, we have $\mathcal{X}_a = \mathcal{Y}_0 = \mathcal{F}$ for all $a \in [1:L]$, for some finite field $\mathcal{F}$ where $|\mathcal{F}| \triangleq F$, and

$$Y_0 = X_1 \oplus X_2 \oplus \cdots \oplus X_L \oplus Z_0 \triangleq \bigoplus_{a=1}^{L} X_a \oplus Z_0, \tag{5}$$

where $\oplus$ is addition in the finite field $\mathcal{F}$, and $Z_0 \in \mathcal{F}$ is an arbitrarily distributed random variable with $H(Z_0)$, and is independent with each channel use. We do not constraint the downlink to take any particular form.

In this paper, we obtain the following:

Theorem 1: The capacity region of the multi-way relay channel with any finite-field uplink and any arbitrary downlink is the set of all non-negative rate tuple $\boldsymbol{r}$, each satisfying

$$r_{\max}^{\Sigma} \leq \log_2 F - H(Z_0), \tag{6}$$

$$r_a^{\Sigma} \leq I(X_0; Y_a), \qquad \text{for all } a \in [1:L], \tag{7}$$

for some pmf $p_{X_0}(x_0)$ on $\mathcal{X}_0$.

The proof for the converse follows from the cut-set argument [11, p. 589], [12], [1]. We present an optimal coding scheme (for achievability) in Section IV.

Remark 1: Theorem 1 includes the results of finite-field multi-way relay channels with independent messages [1] and those with pair-wise common messages [7] as special cases.

B. MIMO AWGN Channel

For a MIMO AWGN channel, each user has M transmit and M receive antennas, and the relay has N transmit and N receive antennas. The received signals of the relay and of user $a \in [1:L]$ are

$$\mathbb{Y}_0 = \sum_{a=1}^{L} \mathbb{H}_{a,0}\mathbb{X}_a + \mathbb{Z}_0 \quad \text{and} \quad \mathbb{Y}_a = \mathbb{H}_{0,a}\mathbb{X}_0 + \mathbb{Z}_a$$

respectively, where $\mathbb{X}_a, \mathbb{Y}_a, \mathbb{Z}_a$ are complex column vectors of length M; $\mathbb{X}_0, \mathbb{Y}_0, \mathbb{Z}_0$ are complex column vectors of length N; $\mathbb{H}_{a,0}$ are $N \times M$ complex matrices; and $\mathbb{H}_{0,a}$ are $M \times N$ complex matrices. We assume that the channel matrices $\mathbb{H}_{\cdot,\cdot}$ have full rank, i.e., $\mathsf{rank}(\mathbb{H}_{\cdot,\cdot}) = \min\{M,N\}$. They are fixed and are known to the users and the relay.

All noise vectors $\{\mathbb{Z}_a\}_{a=0}^{L}$ are zero-mean complex Gaussian vectors with $E[\mathbb{Z}_a\mathbb{Z}_a^{\dagger}] = \sigma_a \mathbf{1}$, for some $\sigma_a > 0$, where $\dagger$ denotes conjugate transpose, and $\mathbf{1}$ is the identity matrix.

We impose a transmit power constraint for all nodes, $E[\mathsf{tr}(\mathbb{X}_a\mathbb{X}_a^{\dagger})] \leq \rho$, where $\mathsf{tr}(\cdot)$ denotes the trace of a matrix.

An achievable rate tuple for the MIMO AWGN channel is thus a function of ρ, which can be written as $\boldsymbol{r}(\rho) = (r_{\mathtt{I}}(\rho) :$

[2] In private message exchange—as opposed to full message exchange—each user sends different (and independent) messages to different receivers.

[3] We simply use messages to denote independent sub-messages of the users.

TABLE I
UPLINK MESSAGE TRANSMISSION

column index	2	3	$\cdots$	L	$(2,3)$	$(2,4)$	$\cdots$	$(L-1,L)$	$\cdots$	$(\mathtt{I})$	$\cdots$	$(2,3,\ldots,L)$
row 1	$\boldsymbol{V}_2$	$\boldsymbol{V}_3$	$\cdots$	$\boldsymbol{V}_L$	$\boldsymbol{V}_{2,3}$	$\boldsymbol{V}_{2,4}$	$\cdots$	$\boldsymbol{V}_{L-1,L}$	$\cdots$	$\boldsymbol{V}_{\mathtt{I}}$	$\cdots$	$\boldsymbol{V}_{2,3,\ldots,L}$
row 2	$\boldsymbol{V}_{\mathbf{1}}$				$\boldsymbol{V}_{\mathbf{1},3}$	$\boldsymbol{V}_{\mathbf{1},4}$				$\boldsymbol{V}_{\mathtt{I}_{2\mapsto 1}}$		$\boldsymbol{V}_{\mathbf{1},3,\ldots,L}$
row 3		$\boldsymbol{V}_{\mathbf{1}}$			$\boldsymbol{V}_{2,\mathbf{1}}$					$\boldsymbol{V}_{\mathtt{I}_{3\mapsto 1}}$		$\boldsymbol{V}_{2,\mathbf{1},\ldots,L}$
$\vdots$												
row L				$\boldsymbol{V}_{\mathbf{1}}$				$\boldsymbol{V}_{L-1,\mathbf{1}}$		$\boldsymbol{V}_{\mathtt{I}_{L\mapsto 1}}$		$\boldsymbol{V}_{2,3,\ldots,\mathbf{1}}$

Note: We have indicated the replaced indices in rows $[2:L]$ in red.

$\mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L])$). In this paper, we derive achievable DOF tuples, defined as

$$\boldsymbol{d} = (d_{\mathtt{I}} : \mathtt{I} \in \mathcal{P}_{\leq L-1}([1:L])) \triangleq \lim_{\rho\to\infty} \frac{\boldsymbol{r}(\rho)}{\log_2 \rho}. \tag{8}$$

Following the notation in (3) and (4), we define $d_a^\Sigma \triangleq \sum_{\mathtt{I}\in\mathcal{W}_a} d_{\mathtt{I}}$, and $d_{\max}^\Sigma \triangleq \max_{a\in[1:L]} d_a^\Sigma$.

Analogous to the capacity region, we find the closure of all achievable DOF tuples, known as the DOF region, as follows:

Theorem 2: The DOF region of the MIMO AWGN multi-way relay channel, with M transmit and M receive antennas at each user, and N transmit and N receive antennas at the relay, is the set of all non-negative DOF tuples $\boldsymbol{d}$, each satisfying

$$d_{\max}^\Sigma \leq \min\{M, N\}. \tag{9}$$

We present the proof of the converse of Theorem 2 in Section V, and achievability in Section VI.

IV. Proof of Achievability of Theorem 1

When the users have only pair-wise common messages, i.e., $W_{\mathtt{I}} = \varnothing$ for all $|\mathtt{I}| > 2$ (i.e., a (sub)message can be known a priori to at most two users), Ong et al. [7] designed an optimal TDMA (time-division multiple access) coding scheme for the uplink where selected users transmit during each time slot, and the relay decodes the modulo addition (in the finite field $\mathcal{F}$) of the transmitted messages. The optimal uplink coding scheme designed therein comprises two components: (i) a message-alignment table to determine which messages should be transmitted in which slots, and (ii) a shuffling step to swap messages in the table to ensure that there are sufficient linearly-independent equations for each user to decode what it wants, when the relay transmits the additions back to the users.

In this paper, we extend the message-alignment table to the general case where a message can be known a priori to any number of users. It turns out that the shuffling step cannot be similarly extended. Hence, we introduce a new method to generate sufficient linearly-independent equations for the users. This method requires grouping of sufficiently long message vectors and rotating the message vectors. We will describe these two steps in detail in the next two sub-sections.

A. Message-Alignment Table

We first injectively map each message $W_{\mathtt{I}} \in [1:2^{nr_{\mathtt{I}}}]$ to a finite-field vector of length $\ell_{\mathtt{I}}$, denoted as $\boldsymbol{V}_{\mathtt{I}} \in \mathcal{F}^{\ell_{\mathtt{I}}}$, where

$$\ell_{\mathtt{I}} = \lceil (nr_{\mathtt{I}})/\log_2 F \rceil. \tag{10}$$

We define $\ell_a^\Sigma \triangleq \sum_{\mathtt{I}\in\mathcal{W}_a} \ell_{\mathtt{I}}$, and $\ell_{\max}^\Sigma \triangleq \max_{a\in[1:L]} \ell_a^\Sigma$.

Without loss of generality (WLOG), assume that user 1 needs to decode the most number of symbols, i.e., $\ell_1^\Sigma = \ell_{\max}^\Sigma$.

Table I depicts our proposed transmission scheme. It contains L rows and $|\mathcal{W}_1|$ columns. It is designed such that the users transmit the messages in each column simultaneously, and the relay decodes the finite-field addition of all messages in each column. The messages are assigned to the cells as follows:

1) In row 1, we put each $\{\boldsymbol{V}_{\mathtt{I}} : \mathtt{I} \in \mathcal{W}_1\}$ (i.e., messages requested by user 1) in one cell. This takes up all $|\mathcal{W}_1|$ cells in row 1. By design, $\mathtt{I}$'s here do not contain 1. We name the column that contains $\boldsymbol{V}_{\mathtt{I}}$ in row 1 column $\mathtt{I}$.
2) In row $a \in [2:L]$ in column $\mathtt{I}$, we assign $\boldsymbol{V}_{\mathtt{I}_{a\mapsto 1}}$ to the cell, where

$$\mathtt{I}_{a\mapsto 1} \triangleq \begin{cases} \mathtt{I} \text{ in which } a \text{ is replaced by } 1, & \text{if } a \in \mathtt{I} \\ \{\}, & \text{otherwise,} \end{cases} \tag{11}$$

where $\boldsymbol{V}_{\{\}} \triangleq \varnothing$.

For simplicity, we first assume that the messages (finite-field vectors) assigned to each column are of equal length.

Using random linear codes of length $n_{\mathtt{I}} = n\ell_{\mathtt{I}}/\ell_{\max}^\Sigma$ for each column $\mathtt{I}$, the relay can decode the finite-field addition of all transmitted message in each column $\mathtt{I}$ if $n_{\mathtt{I}}$ is sufficiently large and if (see, e.g., Ong et al. [1], [7])

$$(\log_2 F^{\ell_{\mathtt{I}}})/n_{\mathtt{I}} = (\ell_{\max}^\Sigma \log_2 F)/n < \log_2 F - H(Z_0). \tag{12}$$

Denote the concatenation of message additions (decoded by the relay) over all $|\mathcal{W}_1|$ columns by $\boldsymbol{U}$. Clearly, $\boldsymbol{U} \in \mathcal{F}^{\ell_1^\Sigma}$, as the relay decodes $\ell_{\mathtt{I}}$ finite-field symbols in each column $\mathtt{I}$.

On the downlink, the relay uses random coding. It chooses some $p_{X_0}(x_0)$ and transmits randomly generated codeword $\boldsymbol{X}_0(\boldsymbol{U}) \in \mathcal{X}_0^n$. From the channel coding theorem [11, Sec 7.7], user 1 can reliably decode $\boldsymbol{U}$ if n is sufficiently large and if

$$(\log_2 F^{\ell_1^\Sigma})/n = (\ell_1^\Sigma \log_2 F)/n < I(X_0; Y_1). \tag{13}$$

Now, for user $a \in [2:L]$, it knows a priori the messages $\boldsymbol{V}_{\mathcal{K}_a} = (\boldsymbol{V}_{\mathtt{I}} : \mathtt{I} \in \mathcal{K}_a)$. Since $\boldsymbol{U}$ is a deterministic function of $(\boldsymbol{V}_{\mathcal{K}_a}, \boldsymbol{V}_{\mathcal{W}_a})$, user a searches over at most $F^{\sum_{\mathtt{I}\in\mathcal{W}_a} \ell_{\mathtt{I}}} = F^{\ell_a^\Sigma}$ candidates of $\boldsymbol{U}$ to determine the correct one. So, any user $a \in [2:L]$ can reliably decode $\boldsymbol{U}$ if [2]

$$(\log_2 F^{\ell_a^\Sigma})/n = (\ell_a^\Sigma \log_2 F)/n < I(X_0; Y_a). \tag{14}$$

After all users have decoded $\boldsymbol{U}$, we need to show the following:

Proposition 1: Each user $a \in [1:L]$ can obtain $\boldsymbol{V}_{\mathcal{W}_a}$ from $\boldsymbol{U}$ and its prior knowledge $\boldsymbol{V}_{\mathcal{K}_a}$.

Proof of Proposition 1: Referring to Table I again, user 1 knows all messages in rows $[2:L]$, and it can decode all messages in row 1 (i.e., $\boldsymbol{V}_{\mathcal{W}_1}$) from $\boldsymbol{U}$.

For user $a \in [2:L]$, consider any column $\mathtt{I} = \mathtt{I}' \cup \{a\}$. By construction, we have $a \notin \mathtt{I}'$, $1 \notin \mathtt{I}'$ (because $1 \notin \mathtt{I}$ for any column $\mathtt{I}$) and $|\mathtt{I}'| \in [0:L-2]$. The messages in column $\mathtt{I}' \cup \{a\}$ are $\boldsymbol{V}_{\mathtt{I}'\cup\{a\}}$ (in row 1), $\mathcal{V}_{\mathtt{I}'\cup\{1\}}$ (in row a), and $\{\boldsymbol{V}_{\mathtt{I}''\cup\{a\}}\}$ where each $\mathtt{I}''$ is formed by replacing one element in $\mathtt{I}'$ by 1. Since user a knows all but $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ in this column, it can decode $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ from the relevant part in $\boldsymbol{U}$. Repeating this, user a can obtain all $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ where $a \notin \mathtt{I}'$.

For $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ where $a \in \mathtt{I}'$, user a knows the message a priori. This means user a can obtain all messages in rows $[2:L]$, which are $\{\boldsymbol{V}_{\mathtt{I}'\cup\{1\}} : |\mathtt{I}'| \in [0:L-2]\}$. Using $\boldsymbol{U}$, it can then decode all messages in row 1 as well.

It is easy to see that each message appears at least once in Table I. Since each user can obtain all messages in the table, it can obtain all its requested messages. ■

We have shown that if (12), (13), and (14) are satisfied, then all users can reliably decode (i.e., with diminishing error probability as n increases) the messages they each request. Note that for any $\psi > 0$, we can always choose a sufficiently large n such that $(\ell_{\mathtt{I}} \log_2 F)/n - r_{\mathtt{I}} < \psi$ while satisfying (10) for all $\mathtt{I}$. This means $(\ell_a^\Sigma \log_2 F)/n$ can be made arbitrarily close to r_a^Σ, and this proves the achievability part of Theorem 1 if all messages in the same column are of the same length.

B. Message Rotation

We will now design a rotation scheme so that Theorem 1 still holds even if the messages are of different lengths.

For (12) to hold, we require that each cell in column $\mathtt{I}$ still contains $\ell_{\mathtt{I}}$ symbols, and that $\boldsymbol{U}$ contains $\ell_1^\Sigma = \ell_{\max}^\Sigma$ symbols. This might not be possible, e.g., if $\ell_1 > \ell_2$, then we cannot fit the entire message $\boldsymbol{V}_1$ in the cell in row 2 in column 2, which has a length of only ℓ_2 symbols.

To rectify this, we now allow the messages in each row $a \in [2:L]$ to *share* their cells. In row a, all cells with assigned messages are in columns $\{\mathtt{I} \in \mathcal{W}_1 : a \in \mathtt{I}\}$. These cells have a total length of $\left(\sum_{\substack{\mathtt{I}\in\mathcal{W}_1 \\ \text{s.t. } a\in\mathtt{I}}} \ell_{\mathtt{I}}\right)$. The messages assigned to these cells are $\{\boldsymbol{V}_{\mathtt{I}_{a\mapsto 1}} : \mathtt{I} \in \mathcal{W}_1$ where $a \in \mathtt{I}\}$, which can be shown to be equal to $\{\boldsymbol{V}_{\mathtt{I}} : \mathtt{I} \in \mathcal{W}_a$ where $1 \in \mathtt{I}\}$, and they have in total $\left(\sum_{\substack{\mathtt{I}\in\mathcal{W}_a \\ \text{s.t. } 1\in\mathtt{I}}} \ell_{\mathtt{I}}\right)$ symbols.

Since we have assumed WLOG that $\sum_{\mathtt{I}\in\mathcal{W}_1} \ell_{\mathtt{I}} \geq \sum_{\mathtt{I}\in\mathcal{W}_a} \ell_{\mathtt{I}}$, it follows that $\sum_{\substack{\mathtt{I}\in\mathcal{W}_1 \\ \text{s.t. } a\in\mathtt{I}}} \ell_{\mathtt{I}} \geq \sum_{\substack{\mathtt{I}\in\mathcal{W}_a \\ \text{s.t. } 1\in\mathtt{I}}} \ell_{\mathtt{I}}$. This means all messages assigned to row a can indeed fit into the designated cells on that row without changing the cell size, by spreading the messages across these cells.

With this, the relay can still reliably decode $\boldsymbol{U}$ (which is the addition of messages in each column, now with the messages being spread) if (12) holds. Since the messages in each row did not change (only the positions changed), all users can still reliably decode $\boldsymbol{U}$ if (13) and (14) hold.

What is left to be shown is that Proposition 1 still holds. Note that the shuffling step [7] used for pair-wise common message cannot be extended to the general case here, as it requires each column to have no more than three messages.

In this paper, we propose a new method: In rows $[2:L]$, instead of sending the messages as they are, we send *rotated* versions of the messages. For each message $\boldsymbol{V}_{\mathtt{I}_{a\mapsto 1}}$, we transmits $\boldsymbol{V}_{\mathtt{I}_{a\mapsto 1}} \odot \mathbf{R}$ instead, where $\mathbf{R} \in \mathcal{F}^{\ell_{\mathtt{I}} \times \ell_{\mathtt{I}}}$ is a fixed rotating matrix unique to each row a and each column $\mathtt{I}$.

This rotation scheme does not affect the decoding of user 1, who can still decode all its required messages in row 1.

Each message in rows $[2:L]$ can be expressed as $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ for some $\mathtt{I}'$ where $0 \leq |\mathtt{I}'| \leq L-2$ and $1 \notin \mathtt{I}'$. From the perspective of user a, each of these messages either appears in row a (if $a \notin \mathtt{I}'$)[4] or is known a priori (if $a \in \mathtt{I}'$). Thus, all messages in rows $[2:L]$ that are unknown to user a appear in row a, and they spread across columns $\{\mathtt{I} : a \in \mathtt{I}\}$. Knowing the messages in row 1 in these columns, user a can decode the messages in row a from the sums in these columns (i.e., the relevant parts in $\boldsymbol{U}$) if the sums are linearly independent.

As the number of messages in Table I is fixed, we can always increase n to get sufficiently long vector length $\ell_{\mathtt{I}}$ for each message $\boldsymbol{V}_{\mathtt{I}}$ (see (10)), so that we can find sufficient number of unique rotating matrices to get linearly-independent equations for each user. To see this, suppose that $\boldsymbol{V}_{1,2} \in \mathcal{F}^\ell$ and $\boldsymbol{V}_{1,3} \in \mathcal{F}^\ell$ align perfectly twice in two columns (this is possible as we allow the messages in each row to spread across the assigned columns). We rotate them such that

$$(\boldsymbol{V}_{1,2} \odot \mathbf{R}_1) \oplus (\boldsymbol{V}_{1,3} \odot \mathbf{R}_2) \oplus \boldsymbol{V}' = \boldsymbol{U}' \in \mathcal{F}^\ell$$
$$(\boldsymbol{V}_{1,2} \odot \mathbf{R}_3) \oplus (\boldsymbol{V}_{1,3} \odot \mathbf{R}_4) \oplus \boldsymbol{V}'' = \boldsymbol{U}'' \in \mathcal{F}^\ell$$

are linearly independent. $\boldsymbol{V}'$ and $\boldsymbol{V}''$ are rotated messages (or parts of) in other rows. Note that we consider the whole ℓ symbol-wise additions as one "equation set". In this example, two equation sets were linearly dependent before the rotation, and choosing one set of rotating matrices made the two equation sets linearly independent. When we increase n (and therefore $\{\ell_{\mathtt{I}}\}$), the number of dependent equation sets remains the same, but the choices of rotation matrices $\{\mathbf{R}\}$ increase.

After decoding messages in row a, user a knows all messages in rows $[2:L]$. It can then decode messages in row 1 in columns $\{\mathtt{I} : a \notin \mathtt{I}\}$. This completes the proof of Theorem 1. ■

Remark 2: Although we can increase the length of the message vectors $\{\ell_{\mathtt{I}}\}$, the function $\boldsymbol{U}$ is still symbol-wise additions (in $\mathcal{F}$, which is fixed for a given channel) of the message vectors. Hence, we cannot simply replace the coding function in Table I with that for network coding [13, Thm 19.20], where the base field must be chosen to be sufficiently large.

V. Proof of the Converse of Theorem 2

It has been shown that for a point-to-point MIMO AWGN channel $\mathbb{Y} = \mathbb{H}\mathbb{X} + \mathbb{Z}$, with M transmit antennas, N receive

[4] For any $\mathtt{I}'$ where $0 \leq |\mathtt{I}'| \leq L-2$ and $1, a \notin \mathtt{I}'$, there must be some column $\mathtt{I} = \mathtt{I}' \cup \{a\}$. So $\boldsymbol{V}_{\mathtt{I}'\cup\{1\}}$ must have been assigned to row a.

antennas, and a transmit power constraint ρ, any DOF is upper bounded as $d = \lim_{\rho\to\infty} \frac{r(\rho)}{\log \rho} \le \min\{M, N\}$, where $r(\rho)$ is an achievable rate for the channel [14].

For the multi-way relay channel, from the cut-set bound [11, Thm 15.10.1], we have $r_a^\Sigma \le I(\mathbb{X}_{[1:L]\setminus\{a\}}; \mathbb{Y}_{\{0,a\}} | \mathbb{X}_{\{0,a\}}) \le h\left(\sum_{i\in[1:L]\setminus\{a\}} \mathbb{H}_{i,0}\mathbb{X}_i + \mathbb{Z}_0\right) - h(\mathbb{Z}_0)$. The last term is the channel capacity of a point-to-point channel $\mathbb{Y}_0 = [\mathbb{H}_{1,0} \cdots \mathbb{H}_{a-1,0}\mathbb{H}_{a+1,0} \cdots \mathbb{H}_{L,0}][\mathbb{X}_1 \cdots \mathbb{X}_{a-1}\mathbb{X}_{a+1} \cdots \mathbb{X}_L]^{\mathrm{T}} + \mathbb{Z}_0$, with $(L-1)M$ transmit and N receive antennas. So,

$$d_a^\Sigma \triangleq \sum_{\mathtt{I}\in\mathcal{W}_a} d_{\mathtt{I}} = \lim_{\rho\to\infty} \frac{r_a^\Sigma}{\log_2 \rho} \le \min\{(L-1)M, N\}, \quad (15)$$

for all $a \in [1:L]$. Also, using the cut-set bound again, we obtain $r_a^\Sigma \le I(\mathbb{X}_0; \mathbb{Y}_a)$, from which we get

$$d_a^\Sigma \le \min\{M, N\}, \quad \text{for all } a \in [1:L], \quad (16)$$

which is equivalent to (9). Given (16), (15) is redundant.

VI. Proof of Achievability of Theorem 2

We now prove that any DOF tuple satisfying (9) is achievable. WLOG, suppose $r_1^\Sigma = r_{\max}^\Sigma$. Let $\delta \triangleq \min\{M, N\}$. For the uplink, we orthogonalize the channel using the Moore-Penrose inverse to obtain δ parallel sub-channels (see, e.g., Jafar and Fakhereddin [14]), and ignore sub-channels with zero gain:

$$Y_0^{(i)} = \sum_{a\in[1:L]} \alpha_a^{(i)} S_a^{(i)} + \tilde{Z}_0^{(i)}, \quad i \in [1:\delta], \quad (17)$$

Here, $S_a^{(i)}$ is the channel input from user a for sub-channel i, $\alpha_a^{(i)}$ is the effective channel gain from user a to the relay on sub-channel i, and $\tilde{Z}_0^{(i)} \sim \mathcal{N}(0, \sigma^{(i)})$ is the effective noise after orthogonalization. Here, the noise $\{\tilde{Z}_0^{(i)}\}$ may be correlated.

We now use our proposed coding scheme in Table I. We set $\mathcal{F} = \{0, 1\}$ so that $\ell_{\mathtt{I}} = nr_{\mathtt{I}}$. We perform appropriate rotations to obtain the required linearly-independent equations for all users. Note that the total *width* of the table is nr_1^Σ bits. We will transmit the messages in the table over n channel uses, where each channel use consists of δ sub-channels (17). We divide the width of the table into δ virtual columns, each having a length of $(nr_1^\Sigma)/\delta$ bits.[5] For virtual column $i \in [1:\delta]$, each user a transmits on sub-channel i the relevant messages (with zero padding if the message length is shorter than the virtual column length) in the virtual column using a lattice code of length n.[6] Let $\mathcal{A}^{(i)}$ be the set of users to transmit in virtual column i. Each user $a \in \mathcal{A}^{(i)}$ transmits with power $E[S_a^{(i)} S_a^{(i)\dagger}] = \min_{b\in\mathcal{A}^{(i)}} \left\{\alpha_b^{(i)} \alpha_b^{(i)\dagger}\right\} \rho \Big/ \left(\delta \alpha_a^{(i)} \alpha_a^{(i)\dagger}\right)$, so that the relay sees the same effective signal-to-noise ratio from these users, while each user satisfies its transmit power ρ. The relay can decode the modulo-lattice addition of the transmitted lattice codewords in virtual column i if [15]

$$\frac{(nr_1^\Sigma)/\delta}{n} < \max\left\{\log_2\left(\frac{1}{|\mathcal{A}^{(i)}|} + \frac{Q_i \rho/\delta}{\sigma^{(i)}}\right), 0\right\}, \quad (18)$$

where $Q_i = \min_{b\in\mathcal{A}^{(i)}} \left\{\alpha_b^{(i)} \alpha_b^{(i)\dagger}\right\}$, and $|\mathcal{A}^{(i)}|$ is the number of non-empty rows in virtual column i (i.e., the number of lattice-codewords being added). This means

$$\begin{aligned} d_1^\Sigma &= \lim_{\rho\to\infty} \frac{r_1^\Sigma}{\log_2 \rho} < \lim_{\rho\to\infty} \frac{\delta}{\log_2 \rho} \log_2\left(\frac{1}{|\mathcal{A}^{(i)}|} + \frac{Q_i \rho/\delta}{\sigma^{(i)}}\right) \\ &= \lim_{\rho\to\infty} \frac{\delta}{\log_2 \rho} \left[\log_2 \rho + \log_2\left(\frac{Q_i}{\delta\sigma^{(i)}}\right)\right] = \delta. \quad (19) \end{aligned}$$

The above inequality is the same for all virtual columns $i \in [1:\delta]$. So, the relay can reliably decode the summation in all virtual columns, $\boldsymbol{U}$, if the DOF tuple satisfies (19).

For the downlink, we use the results from Section IV (where the downlink is an arbitrary channel). User a can decode $\boldsymbol{U}$ on the downlink if (13)–(14) hold. This means,

$$d_a^\Sigma = \lim_{\rho\to\infty} \frac{r_a^\Sigma}{\log_2 \rho} < \min\{M, N\} = \delta, \quad (20)$$

for all $a \in [1:L]$, where the inequality follows from the DOF result for the point-to-point channel.

Recall our assumption that $d_1^\Sigma = d_{\max}^\Sigma$. Combining (19) and (20), we have that a DOF tuple $\boldsymbol{d}$ is achievable if (9) holds. ■

[5] $(nr_1^\Sigma)/\delta$ is an integer for sufficiently large n.

[6] Unlike the finite-field channel where the columns are transmitted using TDMA (one column at a time), here we transmit all virtual columns simultaneously via multiple sub-channels.

References

[1] L. Ong, S. J. Johnson, and C. M. Kellett, "The capacity region of multiway relay channels over finite fields with full data exchange," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3016–3031, May 2011.

[2] L. Ong and S. J. Johnson, "The capacity region of the restricted two-way relay channel with any deterministic uplink," *IEEE Commun. Lett.*, vol. 16, no. 3, pp. 396–399, Mar. 2012.

[3] L. Ong, C. M. Kellett, and S. J. Johnson, "On the equal-rate capacity of the AWGN multiway relay channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5761–5769, Sept. 2012.

[4] T. S. Han, "The capacity region of general multiple-access channel with certain correlated sources," *Inf. Control*, vol. 40, no. 1, pp. 37–60, Jan. 1979.

[5] P. Gács and J. Körner, "Common information is far less than mutual information," *Probl. Control Inf. Theory*, vol. 2, no. 2, pp. 149–162, 1972.

[6] L. Ong, G. Lechner, S. J. Johnson, and C. M. Kellett, "The three-user finite-field multi-way relay channel with correlated sources," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3125–3135, Aug. 2013.

[7] L. Ong, S. J. Johnson, and C. M. Kellett, "Optimal coding functions for pairwise message sharing on finite-field multi-way relay channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, Australia, June 2014, pp. 1866–1871.

[8] K. Lee, N. Lee, and I. Lee, "Achievable degrees of freedom on K-user Y channels," *IEEE Trans. Commun.*, vol. 11, no. 3, pp. 1210–1219, Mar. 2012.

[9] Y. Tian and A. Yener, "Degrees of freedom for the MIMO multi-way relay channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2495–2511, May 2014.

[10] A. Chaaban, K. Ochs, and A. Sezgin, "Simultaneous diagonalization: On the dof region of the K-user MIMO multi-way relay channels," in *Proc. Eur. Wirel.*, Barcelona, Spain, May 14–16 2014, pp. 715–720.

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.

[12] S. Mohajer, C. Tian, and S. N. Diggavi, "On source transmission over deterministic relay networks," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Cairo, Egypt, Jan. 6–8 2010.

[13] R. W. Yeung, *Information Theory and Network Coding*, 1st ed. Springer, 2008.

[14] S. A. Jafar and M. J. Fakhereddin, "Degrees of freedom for the MIMO interference channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, USA, July 9–14 2006, pp. 1452–1456.

[15] U. Erez and R. Zamir, "A modulo-lattice transformation for multiple-access channels," in *Proc. 25th IEEE Conv. Electr. Electron. Eng. Israel*, Tel Aviv, Israel, Dec. 3–5 2008, pp. 836–840.