Fifty-second Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 1 - 3, 2014

Asymmetric Compute-and-Forward: Going Beyond One Hop

Yihua Tan*, Xiaojun Yuan†, Soung Chang Liew*, and Aleksandar Kavcic‡
*Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong, China
†School of Information Science and Technology, ShanghaiTech University, Shanghai, 200031, China
‡Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA

Abstract— **We consider a two-hop relay model in which multiple sources communicate with a single destination via multiple distributed relays. We propose an asymmetric Compute-and-Forward (CoF) scheme that allows lattice coding with different coarse and fine lattices at the sources. The proposed scheme is motivated by the observation that, in an asymmetric CoF system, a higher transmission power at a source does not necessarily translate to a higher achievable information rate. We show that significant performance enhancement can be achieved by optimizing the transmission powers of the sources below their respective budgets. Further, the asymmetric construction of lattice coding allows the relays to conduct different modulo operations to reduce their forwarding rates, thereby supporting higher rates at the sources. However, modulo operations in general incur information loss, and so need to be carefully designed to ensure that the destination can successfully recover the source messages. As such, we propose a novel successive recovering algorithm for decoding at the destination, and establish sufficient conditions to guarantee successful recovery. Numerical results are provided to verify the superiority of our proposed scheme over other schemes.**

I. Introduction

Compute-and-Forward (CoF) was proposed in the seminal work [1] and has attracted much research interest; see [1]–[8] and the references therein. The key idea of CoF is to allow relays to decode linear functions of transmitted messages according to their observed channel coefficients, rather than treating the interference as noise. A nice feature of the CoF scheme in [1] is that channel state information (CSI) is not necessary at the transmitters. However, a closer look indicates that CSI at the transmitters (CSIT) is not needed in [1], because a common lattice code is used at every transmitter side. The use of a common lattice code prevents the scheme from exploiting network asymmetry induced by varying channel gains.

Recently, the work in [2], [3] presented modified CoF schemes with asymmetric lattice coding, in which transmitters employ different coarse and fine lattices. Both [2] and [3] were focused on the first-hop design of relay network. Particularly, the main idea of [3] is that the emitted signal vector of a transmitter does not have to lie in the fine lattice used for lattice encoding. CSIT is useful for precoding to enhance performance in the asymmetric CoF system [3]. However, [3] considered asymmetry in the first hop only, and [2] considered an one-hop model where the receiver has multiple antennas. Not well understood are how the relays should process their received linear combinations and, in particular, how they should optimize the overall system when multiple hops exhibit asymmetry.

In this paper, we propose an asymmetric CoF scheme for relay networks. As a critical difference from [2], [3], the main idea of our approach is based on the observation that, due to the mismatch between the signal combination computed at a relay and the one provided naturally by the channels, transmitting at a higher power in a CoF system does not necessarily yield a higher achievable information rate. In particular, it is desirable to optimize transmit powers of transmitters to below their respective power budgets. As an important part of our new framework, we further study the efficient design of forwarding functions in two-hop relaying. In the conventional CoF scheme [1], every relay takes modulo of its computed combination over a common coarse lattice, so as to reduce the forwarding rate in the next hop. This idea can be extended in a straightforward manner to an asymmetric CoF system (where the sources use different coarse lattices) by letting all relay take modulo over the coarsest coarse lattice [2]. However, there is room for further reduction of forwarding rates (thereby supporting higher rate at the sources, for given second-hop capacity). Specifically, we propose to take different modulo operations at different relays. The challenge is how to ensure the recovery of the original messages at the destination, given the fact that such modulo operations may lead to information loss. To address this issue, we present a successive recovering algorithm and establish sufficient conditions for the successful recovery of the original messages. Numerical results are provided to demonstrate the superiority of our proposed scheme over prior schemes.

II. Preliminaries

A. System Model

Consider a relay network in which L source nodes transmit private messages to a common destination via M intermediate relay nodes. We assume that there is no direct link between any source node and the destination. A two-hop relay protocol is employed. In the first hop, the source nodes transmit signals simultaneously to the relay nodes. In the second hop, the relay nodes transmit signals to the destination. The overall system model is illustrated in Fig. 1. We assume that the two hops are of equal time duration, and each hop consists of n channel uses.

In the first hop, each source and each relay have a single antenna. The channel is a real Gaussian channel with additive

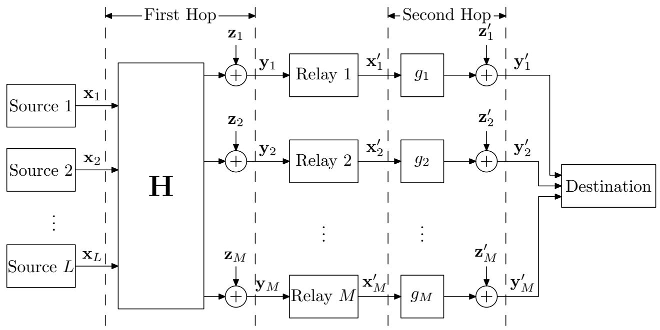

Fig. 1. A diagram representation of the system model.

white Gaussian noise (AWGN), represented as

$$\mathbf{y}_m = \sum_{l=1}^{L} h_{ml}\mathbf{x}_l + \mathbf{z}_m, m = 1, \cdots, M \tag{1}$$

where $\mathbf{x}_l \in \mathbb{R}^{n\times 1}$ is the transmit signal of the l-th source, $\mathbf{y}_m \in \mathbb{R}^{n\times 1}$ is the received signal of the m-th relay, $h_{ml} \sim \mathcal{N}(0,1)$ is the channel coefficient of the link from source l to relay m, and $\mathbf{z}_m \in \mathbb{R}^{n\times 1}$ is an i.i.d. Gaussian noise, $\mathbf{z}_m \sim \mathcal{N}(0, \mathbf{I}_n)$. Denote by $p_l = \frac{1}{n}\|\mathbf{x}_l\|^2$ the average power of source l. Then, the power constraint of source l is given by

$$p_l \le P_l \tag{2}$$

where P_l is the power budget at source l. Further denote the first-hop channel matrix by $\mathbf{H} = [h_{ml}]$ and the channel vector to the m-th relay by $\mathbf{h}_m = [h_{m1}, \cdots, h_{mL}]^T$.

In the second hop, each relay m communicates $\mathbf{x}'_m$ to the destination using an independent scalar Gaussian channel, modeled as

$$\mathbf{y}'_m = g_m\mathbf{x}'_m + \mathbf{z}'_m, m = 1, \cdots, M$$

where $\mathbf{y}'_m \in \mathbb{R}^{n\times 1}$ is the receive signal of the destination from relay m, g_m is the channel coefficient, $\mathbf{x}'_m \in \mathbb{R}^{n\times 1}$ is the signal transmitted by relay m, and $\mathbf{z}'_m \in \mathbb{R}^{n\times 1}$ is an i.i.d. Gaussian noise, $\mathbf{z}'_m \sim \mathcal{N}\left(0, \sigma_1^2\mathbf{I}_n\right)$. The power constraint at relay m is

$$\frac{1}{n}\|\mathbf{x}'_m\|^2 \le P_{R,m}, m = 1, \cdots, M,$$

where $P_{R,m}$ is the power budget at relay m. Note that such independent parallel channels arise in time/frequency division systems. We emphasize that the techniques proposed in this paper can be straightforwardly applied to scenarios with more general second-hop channels, e.g., multiple access channels. Also, for convenience of discussion, we henceforth assume $L = M$, i.e., the number of the source nodes is equal to the number of relay nodes.

B. Nested Lattice Codes

Nested lattice coding is a key technique used in CoF-based relaying. To set the stage for further discussion, we introduce some basic properties of nested lattice codes. A lattice $\Lambda \in \mathbb{R}^n$ is a discrete group under the addition operation, and can be represented as

$$\Lambda = \{\mathbf{s} = \mathbf{G}\mathbf{c} : \mathbf{c} \in \mathbb{Z}^n\}$$

where $\mathbf{G} \in \mathbb{R}^{n\times n}$ is a lattice generating matrix [9]. Let $\mathcal{V}$ denote the fundamental Voronoi region of Λ. Every $\mathbf{x} \in \mathbb{R}^n$ can be uniquely written as $\mathbf{x} = Q_\Lambda(\mathbf{x}) + \mathbf{r}$, where $\mathbf{r} \in \mathcal{V}$ and $Q_\Lambda(\mathbf{x})$ is the nearest lattice point of $\mathbf{x}$ in Λ. Modulo-Λ operation [10] is defined as

$$\mathbf{x} \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}). \tag{3}$$

The second moment per dimension is defined as $\sigma^2(\mathcal{V}) \triangleq \frac{1}{n}\frac{\int_{\mathcal{V}}\|\mathbf{x}\|^2 dx}{V}$, where $V \triangleq \mathrm{Vol}(\mathcal{V})$ is the volume of $\mathcal{V}$. The normalized second moment of Λ is defined as $G(\Lambda) \triangleq \frac{\sigma^2(\mathcal{V})}{V^{2/n}}$.

A coarse lattice Λ_c is nested in a fine lattice Λ_f if $\Lambda_c \subseteq \Lambda_f$. If Λ_c is nested in Λ_f, then

$$[\mathbf{x} \bmod \Lambda_c] \bmod \Lambda_f = \mathbf{x} \bmod \Lambda_f \tag{4}$$

and

$$Q_{\Lambda_c}\left(Q_{\Lambda_f}(\mathbf{x})\right) = Q_{\Lambda_c}(\mathbf{x}) \tag{5}$$

for $\mathbf{x} \in \mathbb{R}^n$.

A lattice codebook can be represented using a nested lattice pair (Λ_f, Λ_c), where $\Lambda_c \subseteq \Lambda_f$, with Λ_c referred to as a shaping lattice and Λ_f as a coding lattice. Denote their Voronoi regions respectively by $\mathcal{V}_f$ and $\mathcal{V}_c$, and the corresponding volumes by V_f and V_c. The generated lattice codebook is

$$\mathcal{C} = \Lambda_f \bmod \Lambda_c \triangleq \Lambda_f \cap \mathcal{V}_c. \tag{6}$$

The rate of this nested lattice code is given by

$$R = \frac{1}{n}\log|\mathcal{C}| = \frac{1}{n}\log\frac{V_c}{V_f}. \tag{7}$$

Moreover, we say that $\Lambda_1, \Lambda_2, \cdots, \Lambda_K$ form a nested lattice chain if $\Lambda_1 \supseteq \Lambda_2 \supseteq \cdots \supseteq \Lambda_K$ [11]. Nested lattice codes with various rates can be constructed by appropriately selecting a pair of coarse and fine lattices from the chain, as will be seen in what follows.

III. Proposed Asymmetric CoF Scheme

In this section, we present an asymmetric CoF scheme for a two-hop relay channel, as illustrated in Fig. 2. The proposed scheme involves asymmetric lattice coding with different fine and coarse lattices. Such asymmetric lattice coding allows performance enhancement based on the CSI.

A. Encoding at the Sources

We use nested lattice codes to encode the messages of the sources. The lattices are generated following Construction A method in [1], [12]. Denote by $\mathbb{F}_\gamma$ the finite field of size γ, where γ is a prime number. Let $\kappa(\cdot)$ be the mapping from the prime-sized finite field $\mathbb{F}_\gamma$ to the corresponding integers $\{0, 1, \cdots, \gamma-1\}$, and $\kappa^{-1}(\cdot)$ be the inverse mapping of $\kappa(\cdot)$. Note that $\kappa(\cdot)$ is sometimes applied to a vector or matrix in an entry-wise manner.

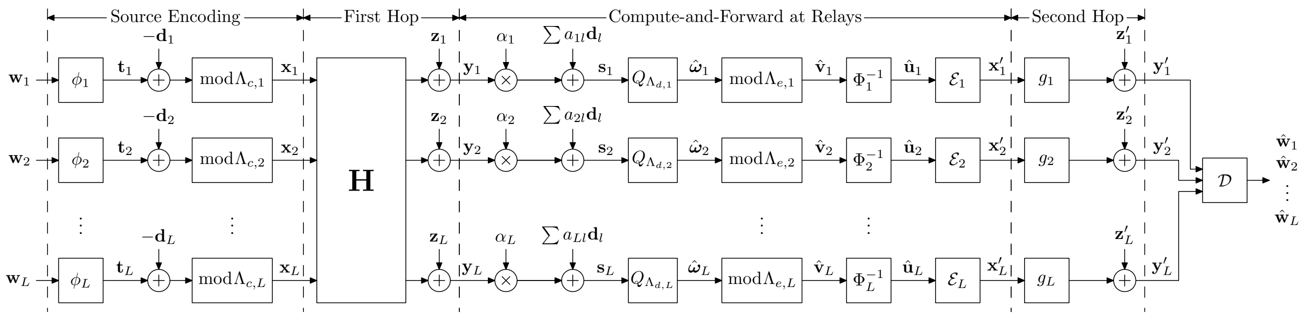

Fig. 2. The diagram of the proposed asymmetric CoF scheme.

We first construct a chain of nested fine lattices following the Construction A method in [1], [12]. Let $\mathbf{G} \in \mathbb{F}_\gamma^{n\times k}$ be a random matrix with i.i.d. elements uniformly drawn over $\mathbb{F}_\gamma$. Denote by $\mathbf{G}_{A,l}$ the first $k_{A,l}$ columns of $\mathbf{G}$, where $k_{A,l} \le k$ is an integer. Define $\mathcal{L}_{A,l} = \left\{\mathbf{G}_{A,l}\mathbf{b} : \mathbf{b} \in \mathbb{F}_\gamma^{k_{A,l}}\right\}$, and construct a lattice $\tilde{\Lambda}_{A,l} = \gamma^{-1}\kappa\left(\mathcal{L}_{A,l}\right) + \mathbb{Z}^n$. Finally, construct a fine lattice as $\Lambda_{A,l} = \mathbf{B}\tilde{\Lambda}_{A,l}$, where $\mathbf{B} \in \mathbb{R}^{n\times n}$ is a lattice generation matrix. In construction, we require $k_{A,1} \ge k_{A,2} \ge \cdots \ge k_{A,L}$, and so the constructed lattices are nested as $\Lambda_{A,1} \supseteq \Lambda_{A,2} \supseteq \cdots \supseteq \Lambda_{A,L}$.

Similarly, we construct a chain of nested coarse lattices $\Lambda_{B,1} \supseteq \Lambda_{B,2} \supseteq \cdots \supseteq \Lambda_{B,L}$, based on the same matrices $\mathbf{G}$ and $\mathbf{B}$, with parameters $k_{B,1} \ge k_{B,2} \ge \cdots \ge k_{B,L}$.

The lattice codebook $\mathcal{C}_l$ for each source l is constructed as follows. We designate for the l-th source a fine lattice $\Lambda_{f,l} = \Lambda_{A,\pi_f(l)}$, and a coarse lattice $\Lambda_{c,l} = \Lambda_{B,\pi_c(l)}$, where $\pi_f(\cdot)$ and $\pi_c(\cdot)$ are two permutation functions that are bijective mappings from $\{1,\cdots,L\}$ to $\{1,\cdots,L\}$. In constructing lattice codebooks, we require $\Lambda_{c,l}$ is nested in $\Lambda_{f,l}$, and thus, $k_{B,\pi_c(l)} < k_{A,\pi_f(l)}$. Then the codebook of source l is $\mathcal{C}_l = \Lambda_{f,l} \cap \mathcal{V}_{c,l}$. Note that the fine lattices and coarse lattices $\{\Lambda_{f,l}, \Lambda_{c,l}\}$ constructed above are good for both AWGN [1] and MSE quantization [10].

We are now ready to describe the encoding function at each source. Let $k_{f,l} = k_{A,\pi_f(l)}$, and $k_{c,l} = k_{B,\pi_c(l)}$. The l-th source draws a vector $\tilde{\mathbf{w}}_l$ over $\mathbb{F}_\gamma$ with length $(k_{f,l} - k_{c,l})$, and zero-pad $\tilde{\mathbf{w}}_l$ with $k_{c,l}$ preceding zeros and $(k - k_{f,l})$ following zeros to form a message:

$$\mathbf{w}_l = \Bigg[\underbrace{0,\cdots,0}_{k_{c,l}},\ \underbrace{\tilde{\mathbf{w}}_l^T}_{k_{f,l}-k_{c,l}},\underbrace{0,\cdots,0}_{k-k_{f,l}}\Bigg]^T \in \mathbb{F}_\gamma^{k\times 1}. \tag{8}$$

The l-th source maps the message $\mathbf{w}_l$ to a lattice codeword in $\mathcal{C}_l$ as

$$\mathbf{t}_l = \phi_l(\mathbf{w}_l) \triangleq \left[\mathbf{B}\gamma^{-1}g\left(\mathbf{G}\mathbf{w}_l\right)\right] \bmod \Lambda_{c,l}. \tag{9}$$

By following the proof of Lemma 5 in [1], it can be shown that $\phi_l(\cdot)$ is a one-to-one mapping. Then, we construct the signal as

$$\mathbf{x}_l = (\mathbf{t}_l - \mathbf{d}_l) \bmod \Lambda_{c,l}, \tag{10}$$

where $\mathbf{d}_l$ is a random dithering signal uniformly distributed in the Voronoi region $\mathcal{V}_{c,l}$ of $\Lambda_{c,l}$. From Lemma 1 of [10], $\mathbf{x}_l$ is uniformly distributed over $\mathcal{V}_{c,l}$. Then, the average power of $\mathbf{x}_l$ is given by [10]

$$p_l = E_{\mathbf{d}_l}\left[\frac{1}{n}\|\mathbf{x}_l\|^2\right] = G\left(\Lambda_{c,l}\right)V_{c,l}^{2/n} \le P_l \tag{11}$$

where $V_{c,l} \triangleq \mathrm{Vol}\left(\mathcal{V}_{c,l}\right)$ and P_l is the power budget of source l in (2).

B. Computing at the Relays

We now consider the relay operations. From (1) and (10), each relay m receives

$$\mathbf{y}_m = \sum_{l=1}^{L} h_{ml}\left(\mathbf{t}_l - \mathbf{d}_l\right) \bmod \Lambda_{c,l} + \mathbf{z}_m \tag{12}$$

and computes a linear combination:

$$\boldsymbol{\omega}_m \triangleq \sum_{l=1}^{L} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right) \tag{13}$$

where $a_{ml}, l = 1,\cdots,L$, are integer coefficients. To this end, the relay first multiplies $\mathbf{y}_m$ by α_m and removes the dithering signals, yielding

$$\begin{aligned}
\mathbf{s}_m &= \alpha_m\mathbf{y}_m + \sum_{l=1}^{L} a_{ml}\mathbf{d}_l \\
&= \alpha_m\sum_{l=1}^{L} h_{ml}\mathbf{x}_l + \alpha_m\mathbf{z}_m + \sum_{l=1}^{L} a_{ml}\mathbf{d}_l \\
&\overset{(a)}{=} \sum_{l=1}^{L}\left(a_{ml}\left(\mathbf{x}_l + \mathbf{d}_l\right) + \theta_{ml}\mathbf{x}_l\right) + \alpha_m\mathbf{z}_m \\
&\overset{(b)}{=} \sum_{l=1}^{L}\Big(a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right) + \theta_{ml}\mathbf{x}_l\Big) + \alpha_m\mathbf{z}_m \\
&= \boldsymbol{\omega}_m + \sum_{l=1}^{L}\theta_{ml}\mathbf{x}_l + \alpha_m\mathbf{z}_m
\end{aligned} \tag{14}$$

where step (a) follows by the definition of $\theta_{ml} \triangleq \alpha_m h_{ml} - a_{ml}$, and step (b) follows from (3) and (10). Then the relay quantizes $\mathbf{s}_m$ using $\Lambda_{d,m}$, yielding

$$\hat{\boldsymbol{\omega}}_m = Q_{\Lambda_{d,m}}\left(\mathbf{s}_m\right) \tag{15}$$

where

$$\Lambda_{d,m} \triangleq \text{fine}\left\{\Lambda_{f,l}, l : a_{ml} \neq 0\right\} \tag{16}$$

denotes the finest lattice in $\{\Lambda_{f,l}, l : a_{ml} \neq 0\}$. Note that $\boldsymbol{\omega}_m \in \Lambda_{d,m}$ is an integer linear combination of $\mathbf{t}_1, \cdots, \mathbf{t}_L$, with some residual dithering signals. This implies that not only the relays but also the destination is required to have the knowledge of $\mathbf{d}_l$ for dither cancellation.

We now determine the rate constraint to ensure the success of computation at relay m. In (14), $\tilde{\mathbf{z}}_m \triangleq \sum_{l=1}^{L} \theta_{ml}\mathbf{x}_l + \alpha_m \mathbf{z}_m$ is an equivalent noise term. The error in decoding $\hat{\boldsymbol{\omega}}_m$ occurs when the equivalent noise $\tilde{\mathbf{z}}_m$ lies outside the Voronoi region of $\Lambda_{d,m}$. Therefore, from [1], the error probability of the computation at relay m goes to zero, i.e.

$$\lim_{n\to\infty} \Pr\left\{\hat{\boldsymbol{\omega}}_m \neq \boldsymbol{\omega}_m\right\} = 0 \tag{17}$$

if

$$V_{f,l} = \text{Vol}\left(\mathcal{V}_{f,l}\right) > \left(2\pi e \max_{m:a_{ml}\neq 0} \tau_m\right)^{n/2} \tag{18}$$

where $\tau_m = \alpha_m^2 + \sum_{l=1}^{L} \left(\alpha_m h_{ml} - a_{ml}\right)^2 p_l$, and $\mathbf{a}_m = [a_{m1}, \cdots, a_{mL}]^T$.

Let $\mathbf{P} = \text{diag}\left(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_L}\right)$. By (7), (11), and (18), the rate of the l-th source is given by

$$r_l = \frac{1}{n} \log \frac{V_{c,l}}{V_{f,l}} \tag{19}$$

$$< \frac{1}{2} \log \left(\frac{p_l}{\max\limits_{m:a_{ml}\neq 0} \left[\alpha_m^2 + \sum_{j=1}^{L} \left(\alpha_m h_{mj} - a_{mj}\right)^2 p_j\right]} \right)$$

$$= \frac{1}{2} \log \left(\frac{p_l}{\max\limits_{m:a_{ml}\neq 0} \left[\alpha_m^2 + \left\|\mathbf{P}\left(\alpha_m \mathbf{h}_m - \mathbf{a}_m\right)\right\|^2\right]} \right). \tag{20}$$

Note that the rate expression in (20) reduces to the rate in Theorem 5 of [1] by letting $p_1 = p_2 = \cdots = p_L$. We will show that, rather than fixing $p_l = P_l$, allowing $p_l < P_l$ can achieve a considerable performance gain.

We now optimize $\{\alpha_m\}$ to obtain better computation rates. Denote $\varphi_m\left(\alpha_m\right) = \alpha_m^2 + \left\|\mathbf{P}\left(\alpha_m \mathbf{h}_m - \mathbf{a}_m\right)\right\|^2$. By letting $\frac{\partial}{\partial \alpha_m} \varphi_m\left(\alpha_m\right) = 0$, we obtain an MMSE coefficient as

$$\alpha_m^{\text{opt}} = \frac{\mathbf{h}_m^T \mathbf{P}\mathbf{P}^T \mathbf{a}_m}{1 + \left\|\mathbf{P}\mathbf{h}_m\right\|^2}. \tag{21}$$

Substituting α_m^{opt} in (20), we obtain

$$r_l < \frac{1}{2} \log \left(\frac{p_l}{\max\limits_{m:a_{ml}\neq 0} \varphi_m\left(\alpha_m^{\text{opt}}\right)} \right)$$

$$= \frac{1}{2} \log \left(\min_{m:a_{ml}\neq 0} \frac{p_l}{\left\|\mathbf{P}\mathbf{a}_m\right\|^2 - \frac{\left\|\mathbf{h}_m^T \mathbf{P}\mathbf{P}^T \mathbf{a}_m\right\|^2}{1+\left\|\mathbf{P}\mathbf{h}_m\right\|^2}} \right) \triangleq \tilde{r}_l. \tag{22}$$

To summarize, a computation rate tuple $(r_1, r_2, \cdots, r_L)$ is achievable in the first hop if $r_l < \tilde{r}_l$, for $l = 1, \cdots L$ (so that (17) is ensured).

C. Forwarding to the Destination

We now present how relay m forwards signal to the destination. Forwarding $\hat{\boldsymbol{\omega}}_m$ directly leads to a high information rate, since $\hat{\boldsymbol{\omega}}_m$, as a linear combination of lattice codewords, may even lie outside of the largest lattice codebook in use. One way to reduce the forwarding rate is to take modulo of $\hat{\boldsymbol{\omega}}_m$ over the coarsest coarse lattice $\Lambda_{B,L}$ [2], referred to as *symmetric modulo approach*. This approach is simple but in general far from optimal. To further reduce forwarding rates, we propose to take modulo over different lattices at different relays, as detailed below.

Define the following modulo operation at relay m:

$$\hat{\mathbf{v}}_m = \hat{\boldsymbol{\omega}}_m \bmod \Lambda_{e,m} \tag{23}$$

where $\Lambda_{e,m} \in \{\Lambda_{c,l}\}$ is the modulo lattice at relay m. We now give an *asymmetric modulo approach* to determine $\Lambda_{e,m}$. Let $\Lambda_{e,m}, m = 1, \cdots, L$, be a permutation of the coarse lattices $\Lambda_{c,l}, l = 1, \cdots, L$, i.e.,

$$\Lambda_{e,m} = \Lambda_{B,\pi_e(m)}, m = 1, \cdots, L \tag{24}$$

where $\pi_e(\cdot)$ is a permutation function of $\{1, \cdots, L\}$.

The $\hat{\mathbf{v}}_m$ obtained by the modulo operation in (23) is a lattice codeword in the m-th relay's equivalent codebook $\mathcal{C}'_m$ generated by the lattice pair $(\Lambda_{d,m}, \Lambda_{e,m})$. Each relay calculates $\hat{\mathbf{u}}_m = \Phi_m^{-1}\left(\hat{\mathbf{v}}_m\right) \in \mathbb{F}_\gamma^k$, where $\Phi_m(\cdot)$ is a mapping from $\mathbb{F}_\gamma^k$ to $\mathcal{C}'_m$ defined in the way of (9), by replacing $\Lambda_{c,l}$ therein with $\Lambda_{e,m}$. Then $\hat{\mathbf{u}}_m$ is re-encoded as $\mathcal{E}_m\left(\hat{\mathbf{u}}_m\right)$ and forwarded to the destination, where $\mathcal{E}_m(\cdot)$ is the re-encoding function of relay m.

By introducing the mod-$\Lambda_{e,m}$ operation, we reduce the forwarding rate at the m-th relay to be

$$R_m \triangleq \frac{1}{n} \log \frac{V_{e,m}}{V_{d,m}}. \tag{25}$$

where $V_{e,m} = \text{Vol}\left(\mathcal{V}_{e,m}\right)$, and $V_{d,m} = \text{Vol}\left(\mathcal{V}_{d,m}\right)$. In general, however, such a modulo operation may lose information, i.e., the destination may be unable to recover $\{\mathbf{w}_l\}$. We say that $\pi_e(\cdot)$ is *feasible* if the destination can correctly recover the source messages $\{\mathbf{w}_l\}$ upon receiving $\{\hat{\mathbf{u}}_m\}$ (under the assumption of $\hat{\boldsymbol{\omega}}_m = \boldsymbol{\omega}_m, \forall m$). We will discuss how to find feasible $\pi_e(\cdot)$ in Subsection III-E.

D. Decoding at the Destination

The decoding at the destination consists of two steps: (i) to decode $\hat{\mathbf{u}}_m$ from $\mathbf{y}'_m$ for $m = 1, \cdots, L$, and (ii) to recover $\{\mathbf{w}_l\}$ from $\{\hat{\mathbf{u}}_m\}$. For step (i), recall that the channels in the second hop are parallel scalar channels. Thus, the destination can decode $\hat{\mathbf{u}}_m$ with a vanishing error probability, provided

$$0 < R_m \leq C_{R,m} = \frac{1}{2} \log\left(1 + |g_m|^2 \frac{P_{R,m}}{\sigma_1^2}\right), m = 1, \cdots, L \tag{26}$$

where $R_m > 0$ is to ensure that every relay forwards a non-trivial linear combination.

We next write R_m as a function of $\{p_l\}$ and $\{r_l\}$. First, from (11), we have

$$V_{c,l} = \left(\frac{p_l}{G\left(\Lambda_{c,l}\right)}\right)^{n/2} = \left(2\pi e \cdot p_l\right)^{n/2} \tag{27}$$

where e is the Euler's number, and $G(\Lambda_{c,l}) = \frac{1}{2\pi e}$ (since $\Lambda_{c,l}$ is good for MSE quantization [10]). Then, by noting $\Lambda_{c,\pi_c^{-1}(l)} = \Lambda_{B,l} = \Lambda_{e,\pi_e^{-1}(l)}, \forall l$, $V_{e,m}$ can be written as a function of $\{p_l\}$:

$$V_{e,m} = V_{c,\pi_c^{-1}(\pi_e(m))} = \left(2\pi e \cdot p_{\pi_c^{-1}(\pi_e(m))}\right)^{n/2}. \quad (28)$$

From (19) and (27), we have

$$V_{f,l} = \frac{V_{c,l}}{2^{nr_l}} = \frac{(2\pi e \cdot p_l)^{n/2}}{2^{nr_l}}. \quad (29)$$

From (16), we have

$$V_{d,m} = \min_{l:a_{ml}\neq 0} \{V_{f,l}\}. \quad (30)$$

Combining (28), (29), and (30), we rewrite (26) as

$$0 < R_m = \frac{1}{2}\log\left(\frac{p_{\pi_c^{-1}(\pi_e(m))}}{\min\limits_{l:a_{ml}\neq 0}\left\{\frac{p_l}{2^{2r_l}}\right\}}\right) \leq C_{R,m} \quad (31)$$

where R_m is a function of $\{p_l\}$ and $\{r_l\}$.

We next focus on step (ii), i.e., to recover $\{\mathbf{w}_l\}$ from $\{\hat{\mathbf{u}}_m\}$. The basic idea is to convert the asymmetric system into a series of symmetric ones (each with a common coarse lattice), so that the method in [1] can be used for message recovery. We start with the following observation on lattice modulo operations: for a linear combination of lattice codewords $\sum a_{ml}\mathbf{t}_l$, we have

$$\left[\sum a_{ml}\mathbf{t}_l\right] \bmod \Lambda_{e,m} \bmod \Lambda_{B,1} \quad (32a)$$
$$= \left[\sum a_{ml}\mathbf{t}_l\right] \bmod \Lambda_{B,1} \quad (32b)$$
$$= \left[\sum a_{ml}\left(\mathbf{t}_l \bmod \Lambda_{B,1}\right)\right] \bmod \Lambda_{B,1} \quad (32c)$$

where $\Lambda_{B,1}$ is the finest coarse lattice used in the system, and (32b) utilizes (4). Note that $(\mathbf{t}_l \bmod \Lambda_{B,1})$ in (32c) is a lattice codeword in the Voronoi region of $\Lambda_{B,1}$. Thus, (32c) represents an effective symmetric system where sources have a common coarse lattice $\Lambda_{B,1}$, and relays conduct symmetric modulo over $\Lambda_{B,1}$. Therefore, $(\mathbf{t}_l \bmod \Lambda_{B,1}), l = 1, \cdots, L$, can be recovered by following the method in [1]. However, the recovered $(\mathbf{t}_l \bmod \Lambda_{B,1}), l = 1, \cdots, L$, are in general not equal to $\mathbf{t}_l$, except the case of $l = \pi_c^{-1}(1)$. This exception is because $\mathbf{t}_{\pi_c^{-1}(1)}$ is a lattice codeword in the Voronoi region of $\Lambda_{B,1}$, and thus $\mathbf{t}_{\pi_c^{-1}(1)} \bmod \Lambda_{B,1} = \mathbf{t}_{\pi_c^{-1}(1)}$. To recover other codewords, we cancel the contribution of the correctly recovered $\mathbf{t}_{\pi_c^{-1}(1)}$ from the combinations $\{\hat{\mathbf{v}}_m\}$, and discard $\hat{\mathbf{v}}_{\pi_e^{-1}(1)}$ (as it is not useful in recovering other lattice codewords). In this way, we obtain a residual asymmetric system, where the $\pi_c^{-1}(1)$-th source and the $\pi_e^{-1}(1)$-th relay are deleted. Then, we can recover $\mathbf{t}_{\pi_c^{-1}(2)}$ in a similar way, and so on and so forth. Finally, we can recover all $\{\mathbf{w}_l\}$.

The above gives a brief description of our proposed algorithm, without considering the impact of the dithering signals. To present the algorithm more rigorously, we introduce the following definitions.

Denote the coefficient matrix $\mathbf{A} = [\mathbf{a}_1, \cdots, \mathbf{a}_L]^T$. We map matrix $\mathbf{A}$ to the corresponding matrix over $\mathbb{F}_\gamma$ using $\kappa(\cdot)$ defined at the beginning of Subsection III-A. To be specific, we define $\mathbf{Q} = \kappa^{-1}(\mathbf{A} \bmod \gamma) \in \mathbb{F}_\gamma^{L\times L}$, where the (i,j)-th element of $\mathbf{Q}$, denoted by $q_{i,j}$, is given by $q_{ij} = \kappa^{-1}(a_{ij} \bmod \gamma)$.

In the residual system at the i-th iteration, the *residual source set* is

$$\mathcal{S}^{(i)} \triangleq \{l | \pi_c(l) \geq i, l \in \{1, \cdots, L\}\}, \quad (33)$$

the *residual relay set* is

$$\mathcal{T}^{(i)} \triangleq \{l | \pi_e(m) \geq i, m \in \{1, \cdots, L\}\}, \quad (34)$$

and the *residual coefficient matrix* $\mathbf{Q}^{(i)} \in \mathbb{F}_\gamma^{(L-i+1)\times(L-i+1)}$ is the submatrix of $\mathbf{Q}$ with the rows indexed by $\mathcal{S}^{(i)}$ and the columns indexed by $\mathcal{T}^{(i)}$. In the above, the superscript "$^{(i)}$" represents the i-th iteration. Define the *effective lattice codebook for the i-th iteration* as $\mathcal{C}_e^{(i)}$, generated by the lattice pair $(\Lambda_{A,1}, \Lambda_{B,i})$. Define a mapping from $\mathbb{F}_\gamma^k$ to $\mathcal{C}_e^{(i)}$ as

$$\psi^{(i)}(\mathbf{b}) \triangleq \left[\mathbf{B}\gamma^{-1}g(\mathbf{G}\mathbf{b})\right] \bmod \Lambda_{B,i} \quad (35)$$

where $\mathbf{b} \in \mathbb{F}_\gamma^k$, and the first $k_{B,i}$ bits of $\mathbf{b}$ are all 0. Denote by $\psi^{-(i)}(\cdot)$ the inverse mapping of $\psi^{(i)}(\cdot)$.

We are now ready to present the *successive recovering algorithm*, as detailed in Algorithm 1 below.

Algorithm 1 Successive Recovering Algorithm

Input: $\hat{\mathbf{u}}_m, m = 1, \cdots, L$
Output: $\hat{\mathbf{w}}_l, l = 1, \cdots, L$
1: **Initialization**: $\hat{\mathbf{v}}_m \leftarrow \Phi_m(\hat{\mathbf{u}}_m)$ for all $m \in \{1, \cdots, L\}$; $\hat{\mathbf{v}}_m^{(1)} \leftarrow \hat{\mathbf{v}}_m$ for all $m \in \{1, \cdots, L\}$.
2: **for** $i = 1$ **to** L:
3: Form a matrix $\hat{\mathbf{U}}^{(i)}$ by stacking $\left(\psi^{-(i)}\left(\hat{\mathbf{v}}_m^{(i)} \bmod \Lambda_{B,i}\right)\right)^T, m \in \mathcal{T}^{(i)}$, in a row-by-row manner.
4: $\bar{\mathbf{w}}_{\pi_c^{-1}(i)} \leftarrow \left(\left[\left(\mathbf{Q}^{(i)}\right)^{-1}\right]_{\eta(i)} \hat{\mathbf{U}}^{(i)}\right)^T$.
5: Recovering: $\hat{\mathbf{t}}_{\pi_c^{-1}(i)} = \psi^{(i)}\left(\bar{\mathbf{w}}_{\pi_c^{-1}(i)}\right)$. $\hat{\mathbf{w}}_{\pi_c^{-1}(i)} \leftarrow \phi_{\pi_c^{-1}(i)}^{-1}\left(\hat{\mathbf{t}}_{\pi_c^{-1}(i)}\right)$.
6: $\tilde{\mathbf{t}}_{\pi_c^{-1}(i)} \leftarrow \hat{\mathbf{t}}_{\pi_c^{-1}(i)} - Q_{\Lambda_{c,\pi_c^{-1}(i)}}\left(\hat{\mathbf{t}}_{\pi_c^{-1}(i)} - \mathbf{d}_{\pi_c^{-1}(i)}\right)$.
7: Cancellation: $\hat{\mathbf{v}}_m^{(i+1)} \leftarrow \left[\hat{\mathbf{v}}_m^{(i)} - a_{m\pi_c^{-1}(i)}\tilde{\mathbf{t}}_{\pi_c^{-1}(i)}\right] \bmod \Lambda_{e,m}$, for $m \in \mathcal{T}^{(i+1)}$.
8: **end for**

Explanations of this algorithm are as follows. In line 3, we construct a symmetric system with the mod-$\Lambda_{B,i}$ operation. In line 4, $\eta(i) \triangleq \sum_{j\in\mathcal{S}^{(i)}} \zeta(i,j)$ is the position index of the $\pi_c^{-1}(i)$-th source in $\mathcal{S}^{(i)}$, where $\zeta(i,j) \triangleq \begin{cases} 1, & \text{if } j \leq \pi_c^{-1}(i) \\ 0, & \text{else} \end{cases}$. Denote by $[\mathbf{Q}]_l$ the l-th row of $\mathbf{Q}$. In lines 4 and 5, we recover source message $\mathbf{w}_{\pi_c^{-1}(i)}$. In lines 6 and 7, we cancel the contribution of $\hat{\mathbf{t}}_{\pi_c^{-1}(i)}$ from $\hat{\mathbf{v}}_m^{(i)}$ to obtain $\hat{\mathbf{v}}_m^{(i+1)}$.

E. Achievable Rates

A sufficient condition to ensure the success of Algorithm 1 (i.e., $\hat{\mathbf{w}}_l = \mathbf{w}_l, l = 1, \cdots, L$) is presented below.

Theorem 1: Assume that $\hat{\boldsymbol{\omega}}_m = \boldsymbol{\omega}_m, m = 1, \cdots, L$, and $\mathbf{Q}^{(i)}, i = 1, \cdots, L$, are of full rank over $\mathbb{F}_\gamma$. Then the output of Algorithm 1 satisfies $\hat{\mathbf{w}}_l = \mathbf{w}_l, l = 1, \cdots, L$.

The proof of Theorem 1 is given in Appendix I. Note that in Theorem 1, for given $\mathbf{Q}$ and $\{p_l\}$, $\left\{\mathbf{Q}^{(i)}\right\}$ is a function of $\mathcal{T}^{(i)}$, and thus a function of $\pi_e(\cdot)$. Therefore, Theorem 1 gives a sufficient condition for the feasibility of $\pi_e(\cdot)$. The following theorem ensures the existence of a feasible $\pi_e(\cdot)$. The proof is given in Appendix II.

Theorem 2: For given $\pi_c(\cdot)$, if $\mathbf{Q}$ is of full rank over $\mathbb{F}_\gamma$, then there exists a mapping $\pi_e(\cdot)$ such that every residual coefficient matrix $\mathbf{Q}^{(i)}$ is of full rank over $\mathbb{F}_\gamma$.

A feasible $\pi_e(\cdot)$ is in general not unique. Thus, we need to search over all feasible $\pi_e(\cdot)$ in system optimization.

We are now ready to present the achievable rates of the proposed scheme. We say that a rate tuple $(r_1, r_2, \cdots, r_L)$ is achievable if the destination recovers the original messages $\{\mathbf{w}_l\}$ correctly with vanishing error probability as $n \to \infty$. We have the following theorem.

Theorem 3: For given $\mathbf{H}$, $\mathbf{A}$, and $\{C_{R,m}\}$, a transmission rate tuple $(r_1, r_2, \cdots, r_L)$ is achievable if there exist $\{p_l\}$ and $\pi_e(\cdot)$, such that the following constraints are met:

- power constraints in (11): $p_l \leq P_l, \forall l$,
- computation constraints in (22): $r_l < \tilde{r}_l, \forall l$,
- forwarding rate constraints in (31): $0 < R_m \leq C_{R,m}$,
- recovery constraints: every $\mathbf{Q}^{(i)}$ is of full rank over $\mathbb{F}_\gamma$.

The proof of Theorem 3 is straightforward by combining (22), (31), and Theorem 1.

IV. Sum-Rate Maximization

In this section, we consider optimizing the achievable sum rate $\sum_{l=1}^{L} r_l$ for the proposed asymmetric CoF scheme. A centralized node is assumed to acquire all the knowledge of $\mathbf{H}$, $\{C_{R,m}\}$, and $\{P_l\}$. This centralized node informs each source l of lattice pair $(\Lambda_{f,l}, \Lambda_{c,l})$, and each relay m of quantization lattice $\Lambda_{d,m}$ and the modulo lattice $\Lambda_{e,m}$.

A. Problem Formulation

From Theorem 3, the sum rate maximization problem can be formulated as

$$\max_{\substack{\mathbf{A},\{p_l\},\\ \{r_l\},\pi_e(\cdot)}} \quad \sum_{l=1}^{L} r_l \tag{36a}$$

$$\text{s.t.} \quad p_l \leq P_l, \forall l, \tag{36b}$$

$$r_l < \frac{1}{2}\log\left(\min_{m:a_{ml}\neq 0} \frac{p_l}{\|\mathbf{P}\mathbf{a}_m\|^2 - \frac{\|\mathbf{h}_m^T\mathbf{P}\mathbf{P}^T\mathbf{a}_m\|^2}{1+\|\mathbf{P}\mathbf{h}_m\|^2}}\right), \forall l, \tag{36c}$$

$$0 < \frac{1}{2}\log\left(\frac{p_{\pi_c^{-1}(\pi_e(m))}}{\min\limits_{l:a_{ml}\neq 0}\left\{\frac{p_l}{2^{2r_l}}\right\}}\right) \leq C_{R,m}, \forall m, \tag{36d}$$

$$\text{rank}\left(\mathbf{Q}^{(i)}\right) = L - i + 1, i = 1, \cdots, L. \tag{36e}$$

The above problem is non-convex, and is in general difficult to find the optimal solution. Here we present a sub-optimal solution as follows. To optimize $\{p_l\}$, we use brute-force search—compute N_{brute} equal intervals for each p_l. For given $\{p_l\}$, we apply LLL algorithm [6] to find a sub-optimal matrix $\mathbf{A}$. For given $\mathbf{A}$ and $\{p_l\}$, we search for all permutations $\pi_e : \{1, \cdots, L\} \mapsto \{1, \cdots, L\}$. For given $\mathbf{A}$, $\{p_l\}$, and $\pi_e\{\cdot\}$, we find the largest $\{r_l\}$ that satisfies (36c) and (36d). Finally we calculate the sum rate in (36a). There may be multiple feasible $\pi_e\{\cdot\}$ and thus multiple sum rates, and we just need to choose the largest one. Note that, since LLL algorithm outputs multiple vectors for each relay, we select one vector for each relay m as integer coefficient $\mathbf{a}_m$, such that the obtained $\mathbf{Q}$ is of full rank over $\mathbb{F}_\gamma$. Therefore, by Theorem 2, there exists a $\pi_e(\cdot)$ such that $\left\{\mathbf{Q}^{(i)}\right\}$ are all of full rank.

The gap from optimality in the above sub-optimal algorithm only comes from the finite precision in brute-force search for $\{p_l\}$, and sub-optimality of LLL algorithm.

B. Numerical Results

We now present numerical results to demonstrate the proposed asymmetric CoF scheme. In simulation, the following settings are employed: $L = 2$; $P_l = P, \forall l$; $N_{\text{brute}} = 100$; $\sigma_1^2 = 1$, i.e., $\mathbf{z}'_m \sim \mathcal{N}(0, \mathbf{I}_n)$; $P_{R,m} = 0.25P, \forall m$. The following three schemes are simulated for comparison: (i) the original CoF in [1], (ii) the asymmetric CoF with symmetric modulo approach, and (iii) the proposed asymmetric CoF with asymmetric modulo approach.

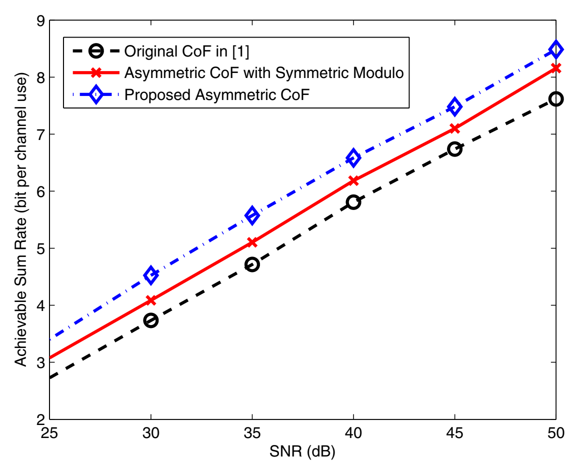

Fig. 3. Achievable sum rate of the proposed asymmetric CoF scheme and two other schemes in the considered two-hop relay channel.

Fig. 3 shows that the asymmetric CoF with symmetric modulo approach achieves a gain of about 2 dB over the original CoF [1], demonstrating the importance of the optimization on source power. Our proposed asymmetric CoF has a gain of about 2.5 dB over the asymmetric CoF with symmetric modulo, demonstrating the effectiveness of our asymmetric modulo approach. Optimization on source power and the asymmetric modulo approach amount to a gain of 4.5 dB.

V. Conclusions

In this paper, we studied communication mechanisms for a two-hop relay network involving multiple sources, multiple relays, and a single destination. We proposed an asymmetric CoF scheme that allows different lattice coding at the sources, thereby allowing unequal transmission powers of the sources. Further, the asymmetric construction of lattice coding allows the relays to conduct asymmetric modulo operations to reduce their forwarding rates. In this regard, we proposed a successive recovering algorithm to ensure that the destination can successfully recover the source messages. Numerical results demonstrate that, by optimizing on source power and conducting asymmetric modulo operations at the relays, our asymmetric CoF scheme achieves a significant power gain, as compared with the original CoF scheme in [1].

Appendix I
Proof of Theorem 1

By assumption, we have $\hat{\boldsymbol{\omega}}_m = \boldsymbol{\omega}_m$, for $m = 1, \cdots, L$. Thus, substituting (13) into (23), we obtain

$$\hat{\mathbf{v}}_m = \left[\sum_{l=1}^{L} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right)\right] \bmod \Lambda_{e,m}. \quad (37)$$

We next show that in the i-th iteration $\hat{\mathbf{v}}_m^{(i)}$ can be written as

$$\hat{\mathbf{v}}_m^{(i)} = \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right)\right] \bmod \Lambda_{e,m} \quad (38)$$

for $m \in \mathcal{T}^{(i)}$, and that exactly one message of $\{\mathbf{w}_l\}$ is restored in each iteration. We prove by induction. From (33) and $\hat{\mathbf{v}}_m^{(1)} = \hat{\mathbf{v}}_m$ (in the initialization of Algorithm 1), we immediately see that (38) holds for $i = 1$. Now suppose that (38) holds for the i-th iteration. We aim to show that (38) also holds for the $(i+1)$-th iteration.

By the definition of $\mathcal{S}^{(i)}$ and $\mathcal{T}^{(i)}$, $\Lambda_{B,i} = \Lambda_{c,\pi_c^{-1}(i)}$ is the finest in $\left\{\Lambda_{c,l} | l \in \mathcal{S}^{(i)}\right\}$, and also the finest in $\left\{\Lambda_{e,m} | m \in \mathcal{T}^{(i)}\right\}$. Then

$$\begin{aligned}
&\hat{\mathbf{v}}_m^{(i)} \bmod \Lambda_{B,i} \\
&= \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right)\right] \bmod \Lambda_{e,m} \bmod \Lambda_{B,i} \\
&= \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right)\right] \bmod \Lambda_{B,i} \\
&= \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\mathbf{t}_l\right] \bmod \Lambda_{B,i}. \quad (39)
\end{aligned}$$

To construct a symmetric system, we further write (39) as

$$\begin{aligned}
&\hat{\mathbf{v}}_m^{(i)} \bmod \Lambda_{B,i} \\
&= \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\left(\mathbf{t}_l \bmod \Lambda_{B,i}\right)\right] \bmod \Lambda_{c,\pi_c(i)} \\
&= \left[\sum_{l\in\mathcal{S}^{(i)}} a_{ml}\bar{\mathbf{t}}_l^{(i)}\right] \bmod \Lambda_{B,i} \quad (40)
\end{aligned}$$

where $\bar{\mathbf{t}}_l^{(i)} \triangleq \mathbf{t}_l \bmod \Lambda_{B,i}$ is a codeword in the effective lattice codebook $\mathcal{C}_e^{(i)}$ defined in Subsection III-D. That is, all $\bar{\mathbf{t}}_l^{(i)}$ can be seen as from a common codebook $\mathcal{C}_e^{(i)}$. Note that

$$\bar{\mathbf{t}}_{\pi_c^{-1}(i)}^{(i)} = \mathbf{t}_{\pi_c^{-1}(i)} \bmod \Lambda_{B,i} = \mathbf{t}_{\pi_c^{-1}(i)} \quad (41)$$

since $\Lambda_{B,i} = \Lambda_{c,\pi_c^{-1}(i)}$.

Define a *virtual message* $\bar{\mathbf{w}}_l^{(i)} = \psi^{-(i)}\left(\bar{\mathbf{t}}_l^{(i)}\right)$, for $l = 1, \cdots, L$. By (40), (35), and Lemma 6 in [1], we have

$$\sum_{l\in\mathcal{S}^{(i)}} q_{ml}\bar{\mathbf{w}}_l^{(i)} = \psi^{-(i)}\left(\hat{\mathbf{v}}_m^{(i)} \bmod \Lambda_{B,i}\right). \quad (42)$$

Form the matrix $\bar{\mathbf{W}}^{(i)}$ by stacking $\bar{\mathbf{w}}_m^{(i)T}, m \in \mathcal{S}^{(i)}$, row by row. Similarly, form the matrix $\hat{\mathbf{U}}^{(i)}$ by stacking $\left(\psi^{-(i)}\left(\hat{\mathbf{v}}_m^{(i)} \bmod \Lambda_{B,i}\right)\right)^T, m \in \mathcal{T}^{(i)}$. We can write (42) as

$$\mathbf{Q}^{(i)}\bar{\mathbf{W}}^{(i)} = \hat{\mathbf{U}}^{(i)}, \quad (43)$$

which is a matrix equation over $\mathbb{F}_\gamma^k$. The destination can obtain

$$\bar{\mathbf{W}}^{(i)} = \left(\mathbf{Q}^{(i)}\right)^{-1}\hat{\mathbf{U}}^{(i)} \quad (44)$$

where $\mathbf{Q}^{(i)}$ is of full rank by assumption. We have $\bar{\mathbf{w}}_{\pi_c^{-1}(i)}^{(i)} = \left(\left[\left(\mathbf{Q}^{(i)}\right)^{-1}\right]_{\eta(i)}\hat{\mathbf{U}}^{(i)}\right)^T$. Note that the $\pi_c^{-1}(i)$-th source is at the $\eta(i)$-th position of the residual system since some sources are already deleted in the i-th iteration.

Then by $\bar{\mathbf{t}}_{\pi_c^{-1}(i)}^{(i)} = \psi^{(i)}\left(\bar{\mathbf{w}}_{\pi_c^{-1}(i)}^{(i)}\right)$ and (41), we obtain the lattice codeword from the $\pi_c(i)$-th source

$$\mathbf{t}_{\pi_c^{-1}(i)} = \psi^{(i)}\left(\bar{\mathbf{w}}_{\pi_c^{-1}(i)}^{(i)}\right).$$

The destination recover $\mathbf{w}_{\pi_c^{-1}(i)}$ as

$$\hat{\mathbf{w}}_{\pi_c^{-1}(i)} = \phi_{\pi_c^{-1}(i)}^{-1}\left(\mathbf{t}_{\pi_c^{-1}(i)}\right) = \mathbf{w}_{\pi_c^{-1}(i)}.$$

Thus, the message of the $\pi_c^{-1}(i)$-th source is correctly recovered.

Then the destination calculates

$$\tilde{\mathbf{t}}_{\pi_c^{-1}(i)} = \mathbf{t}_{\pi_c^{-1}(i)} - Q_{\Lambda_{B,i}}\left(\mathbf{t}_{\pi_c^{-1}(i)} - \mathbf{d}_{\pi_c^{-1}(i)}\right) \quad (45)$$

and cancel the contribution of $\mathbf{t}_{\pi_c^{-1}(i)}$ and $\mathbf{d}_{\pi_c^{-1}(i)}$ from $\hat{\mathbf{v}}_m^{(i)}$ to obtain

$$\hat{\mathbf{v}}_m^{(i+1)} = \left[\hat{\mathbf{v}}_m^{(i)} - a_{m\pi_c^{-1}(i)}\tilde{\mathbf{t}}_{\pi_c^{-1}(i)}\right] \bmod \Lambda_{e,m} \quad (46)$$

for $m \in \mathcal{T}^{(i+1)}$. By noting that $\mathcal{S}^{(i+1)} = \mathcal{S}^{(i)} \setminus \left\{\pi_c^{-1}(i)\right\}$ and $\mathcal{T}^{(i+1)} = \mathcal{T}^{(i)} \setminus \left\{\pi_e^{-1}(i)\right\}$, we have

$$\hat{\mathbf{v}}_m^{(i+1)} = \left[\sum_{l \in \mathcal{S}^{(i+1)}} a_{ml}\left(\mathbf{t}_l - Q_{\Lambda_{c,l}}\left(\mathbf{t}_l - \mathbf{d}_l\right)\right)\right] \bmod \Lambda_{e,m} \tag{47}$$

for $m \in \mathcal{T}^{(i+1)}$, establishing (38) by induction. This concludes the proof of Theorem 1.

APPENDIX II
PROOF OF THEOREM 2

We prove by constructing a sequence of $\mathbf{Q}^{(i)}$. By assumption, $\mathbf{Q}$ is of full rank, so $\mathbf{Q}^{(1)}$. Recall that $\mathcal{S}^{(i)}$ and $\mathcal{T}^{(i)}$ can be rewritten as

$$\mathcal{S}^{(i)} = \left\{\pi_c^{-1}(i), \pi_c^{-1}(i+1), \cdots, \pi_c^{-1}(L)\right\} \tag{48}$$

and

$$\mathcal{T}^{(i)} = \left\{\pi_e^{-1}(i), \pi_e^{-1}(i+1), \cdots, \pi_e^{-1}(L)\right\}. \tag{49}$$

From (48) and (49), we see that $\mathbf{Q}^{(i+1)}$ can be obtained by deleting one row and one column from $\mathbf{Q}^{(i)}$.

Suppose $\mathbf{Q}^{(i)} \in \mathbb{F}_\gamma^{(L-i+1)\times(L-i+1)}$ is of full rank, and we want to find a $\mathbf{Q}^{(i+1)} \in \mathbb{F}_\gamma^{(L-i)\times(L-i)}$ of full rank. Since $\pi_c(\cdot)$ is given, we delete the corresponding column of $\mathbf{Q}^{(i)}$, yielding a matrix $\tilde{\mathbf{Q}}^{(i)}$ of rank $(L-i)$. From linear algebra, we can always delete one row of $\tilde{\mathbf{Q}}^{(i)}$ to obtain $\mathbf{Q}^{(i)}$, so that $\mathbf{Q}^{(i+1)}$ is of full rank $(L-i)$. We set a value of $\pi_e(\cdot)$ according to the index of the deleted row.

Repeat the above process by running from $i=1$ to $i=L$, which concludes the proof of Theorem 2.

REFERENCES

[1] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[2] V. Ntranos, V. R. Cadambe, B. Nazer, and G. Caire, "Asymmetric compute-and-forward," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2013, pp. 1174–1181.

[3] J. Zhu and M. Gastpar, "Asymmetric compute-and-forward with CSIT," *arXiv preprint arXiv:1401.3189*, 2014.

[4] U. Niesen and P. Whiting, "The degrees of freedom of compute-and-forward," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5214–5232, 2012.

[5] X. Yuan, T. Yang, and I. Collings, "Multiple-input multiple-output two-way relaying: A space-division approach," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6421–6440, Oct. 2013.

[6] A. Sakzad, J. Harshan, and E. Viterbo, "Integer-forcing MIMO linear receivers based on lattice reduction," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 4905–4915, 2013.

[7] Z. Fang, X. Yuan, and X. Wang, "Towards the asymptotic sum capacity of the mimo cellular two-way relay channel," to appear in IEEE Trans. Signal Process. Available online: http://arxiv.org/abs/1403.6703.

[8] T. Yang, X. Yuan, L. Ping, I. B. Collings, and J. Yuan, "A new physical-layer network coding scheme with eigen-direction alignment precoding for mimo two-way relaying," *IEEE Trans. Commun.*, vol. 61, no. 3, March 2013.

[9] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," in *Proceedings of the 27th Convention of Electrical & Electronics Engineers in Israel (IEEEI)*, 2012, pp. 1–12.

[10] U. Erez and R. Zamir, "Achieving 1/2log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.

[11] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5488–5494, 2010.

[12] E. Bannai, *Sphere packings, lattices and groups*. Springer, 1999, vol. 290.