Inverse Compute-and-Forward: Extracting Messages from Simultaneously Transmitted Equations

Yiwei Song*, Natasha Devroye*, and Bobak Nazer†
*ECE Department, University of Illinois at Chicago, Chicago, IL 60607
† ECE Department, Boston University, Boston, MA 02215

***Abstract*—We consider the transmission of independent messages over a Gaussian relay network with interfering links. Using the compute-and-forward framework, relays can efficiently decode equations of the transmitted messages. The relays can then send their collected equations to the destination, which solves for its desired messages. Here, we study a special case of the inverse compute-and-forward problem: transmitting the equations to a single destination over a multiple-access channel. We observe that if the underlying messages have unequal rates, the set of possible values of an equation is constrained by the value of the other equations. We use this fact to improve the rate region for downloading equations. Interestingly, the rate region achieved over relay networks with interfering links using a combination of compute-and-forward and inverse compute-and-forward is larger than the best rate region achievable in the absence of interfering links. This verifies that interference may be used to beneficially "mix" messages over a wireless network.**

I. Introduction

Motivation. Of central importance in understanding how to communicate over wireless multi-hop relay networks is the question of how to deal with interference. A canonical example of such a network is shown in Fig. 1. There, two transmitters communicate with a single destination over an additive white Gaussian noise (AWGN) network with the help of two relays. We focus on the case where the messages have unequal rates and the relays have unequal powers. The goal is to exploit the cross-channel gains so that the higher rate message can benefit from the relay with more power.

To be more specific, in the compute-and-forward (CF) framework for Gaussian multi-hop wireless relay networks, intermediate relay nodes decode a linear combination, or equation, of the transmitted codewords by exploiting the noisy linear combinations provided by the channel. Through the use of nested lattice codes, it was shown that decoding linear combinations may be done at higher rates than decoding the individual codewords – one of the key benefits of using structured rather than random i.i.d. codewords [1]. While the decoding of message equations has been tackled, ultimately destination nodes may wish to decode individual messages. Thus, in the final hop of wireless Gaussian networks, one may either transmit and decode the message equations directly, after which the destination inverts the equations to obtain the original messages, or one may attempt to decode the original messages directly from the simultaneously transmitted combinations. We demonstrate the latter – an inverse compute-and-forward (ICF) strategy that outperforms the forwarding of message equations for unequal rates.

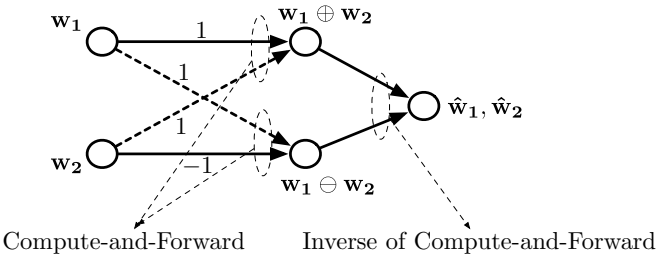

Fig. 1. Canonical example of CF and ICF.

Related Work. Nested lattice codes [2]–[5] play a central role in compute-and-forward framework, where their particular structural and group properties allow for linear combinations of lattice codewords to be decoded at higher rates than decoding the individual codewords. This property has been exploited in several other multi-user scenarios, including two-way relay channels [6]–[9], interference channels [10], [11], Gaussian relay networks [1], [12], [13], distributed dirty paper coding [14], distributed Gaussian source coding [15], and for canceling known interference in multi-hop channels [16].[1] Several groups have studied the broadcast phase of the two-way relay channel [17]–[20], which can be viewed as a special case of our considerations.

Contributions. We study the inverse-compute-and-forward problem and present a binning strategy for extracting the messages $\mathbf{w}_1, \mathbf{w}_2$ over a multiple access channel (MAC) from the equations $a_{11}\mathbf{w}_1 \oplus a_{12}\mathbf{w}_2$ and $a_{21}\mathbf{w}_1 \oplus a_{22}\mathbf{w}_2$. This problem can also be recast as MAC with a common message for which the capacity is known [21]. We then combine this rate region with that of compute-and-forward for the canonical network example of Fig. 1 to show that the presence of the two interfering dotted links can be beneficially exploited to handle the asymmetry in the message rates and relay powers.

II. Problem Statement

We present definitions for the inverse-compute-and-forward framework for a network with two transmitters, two relays, and a single destination. Later, we will briefly delve into extensions to larger networks.

Each transmitter (indexed by $\ell = 1, 2$) has an independent message w_ℓ that is uniformly distributed over $\{1, 2, \cdots, 2^{nR_\ell}\}$

[1] In this work, our achievability scheme does not rely on nested lattice codes but lattices are implicitly used to send equations of messages to the relays.

where n is the number of channel uses and $R_\ell \geq 0$ is the message rate. To use the compute-and-forward framework, we need to map these messages onto a finite field. Let $\mathbf{w}_\ell \in \mathbb{F}_q^{k_\ell}$ be the resulting message vectors where q is a prime and $k_\ell = \frac{nR_\ell}{\log_2 q}$. We zero-pad the shorter of the two message vectors to the length of the longer one, $k_{\text{MAX}} = \max(k_1, k_2)$, to ensure that sums of these vectors are well-defined. Similarly, let $R_{\text{MAX}} = \max(R_1, R_2)$ and $R_{\text{MIN}} = \min(R_1, R_2)$.

Each relay is assumed to have successfully decoded a linear equation of the message vectors, $\mathbf{u}_\ell = a_{\ell 1}\mathbf{w}_1 \oplus a_{\ell 2}\mathbf{w}_2$, where the coefficients are also elements of the finite field, $a_{\ell 1}, a_{\ell 2} \in \mathbb{F}_q$, and $\oplus$ denotes finite field addition. The messages can be recovered from the equations if and only if the equations are linearly independent or, equivalently, the matrix of coefficients $\mathbf{A} = \{a_{\ell m}\}$ is full rank over $\mathbb{F}_q$. We assume this is the case throughout the paper.

The relays encode their equations into channel inputs that are sent towards the destination over a memoryless Gaussian multiple-access channel. The encoder, $\mathcal{E}_\ell : \mathbb{F}_q^{k_{\text{MAX}}} \to \mathbb{R}^n$, at each relay maps the equation $\mathbf{u}_\ell$ into a sequence of n channel inputs, $X_\ell^n = (X_\ell[1], X_\ell[2], \cdots, X_\ell[n])$, that obey an expected[2] power constraint, $E\left[|X_\ell|^2\right] \leq S_\ell$. The channel output observed at the destination is a sum of the channel inputs plus i.i.d. Gaussian noise, $Y[i] = X_1[i] + X_2[i] + Z[i]$, where $Z[i]$ is i.i.d. according to $\mathcal{N}(0,1)$.

At the destination, the decoder, $\mathcal{D} : \mathbb{R}^n \to \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2}$ makes estimates $\hat{\mathbf{w}}_1$ and $\hat{\mathbf{w}}_2$ of the original messages $\mathbf{w}_1$ and $\mathbf{w}_2$ from then channel output Y^n. We say that a rate pair (R_1, R_2) is achievable if, for any $\epsilon > 0$ and n large enough, there exist encoders, $\mathcal{E}_1, \mathcal{E}_2$, and a decoder, $\mathcal{D}$, such that

$$\Pr((\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2) \neq (\mathbf{w}_1, \mathbf{w}_2)) < \epsilon \ . \tag{1}$$

Finally, we define $C(x) := \frac{1}{2}\log_2(1+x)$.

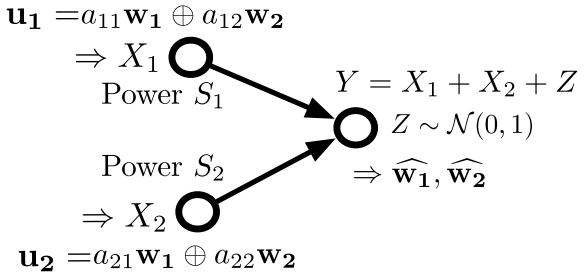

Fig. 2. Channel model for two message inverse-compute-and-forward.

III. Approach I: Allowable Equations

In this section, we develop a simple binning scheme for sending the equations to the receiver. Note that this method produces independent channel inputs across transmitters. In Section IV, we demonstrate that the transmitters in fact share a common message which can be used to generate dependent inputs.

[2]We can easily accommodate a block power constraint at the expense of an extra step in the proof.

A. Cardinality Bound

We now relate the number of messages to the number of possible equations, which will be useful in union bounding the error events in the achievability proof. Recall that the matrix $\mathbf{A}$ is assumed to be full rank, which means that $(\mathbf{w}_1, \mathbf{w}_2)$ can be uniquely determined from $(\mathbf{u}_1, \mathbf{u}_2)$. To simplify the description of the rate region, we consider the case where all coefficients are non-zero, $a_{\ell m} \neq 0$. Since each equation $\mathbf{u}_\ell$ is a modulo-sum of two messages, it can take on exactly $2^{nR_{\text{MAX}}}$ values. This seems to imply that the relays each need to send R_{MAX} bits per channel user to the destination. If $R_1 \neq R_2$, then this is wasteful as we are using more rate than the sum rate of the original messages, $2R_{\text{MAX}} > R_1 + R_2$. Our scheme circumvents this problem by taking advantage of the fact that if one equation is fixed, the number of possible values for the other equation decreases.

Let $\mathcal{M}_{\mathbf{A}}(U_1, U_2)$ denote the set of all possible equation values under the coefficient matrix $\mathbf{A}$,

$$\mathcal{M}_{\mathbf{A}}(U_1, U_2) = \Big\{(\mathbf{u}_1, \mathbf{u}_2) : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2, \ \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2, \ \text{for some } \mathbf{w}_1, \mathbf{w}_2\Big\} \ . \tag{2}$$

Additionally, let $\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2)$ denote the set of possible equations at relay 1 given that the equation at relay 2 is equal to $\mathbf{u}_2$,

$$\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2) = \Big\{\mathbf{u}_1 : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2 \text{ for some } \mathbf{w}_1, \mathbf{w}_2 \text{ satisfying } \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2\Big\} \ ,$$

and similarly define $\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1)$. In deriving an achievable rate region for inverse-compute-and-forward, we will work with a union bound over the sets defined above. We now derive their cardinality.

Lemma 1: **Cardinality lemma.** The set of allowable equations $\mathcal{M}_{\mathbf{A}}(U_1, U_2)$ and the set of conditionally allowable equations $\mathcal{M}_{\mathbf{A}}(U_\ell|\mathbf{u}_m)$ have the following cardinalities:

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2)| = 2^{n(R_1+R_2)}$$
$$|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2)| = 2^{nR_{\text{MIN}}}$$
$$|\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1)| = 2^{nR_{\text{MIN}}} \ .$$

Proof: First, we consider the cardinality of $\mathcal{M}_{\mathbf{A}}(U_1, U_2)$. The pair of equations for $\mathbf{u}_1$ and $\mathbf{u}_2$ can be written in matrix form as $[\mathbf{u}_1 \ \mathbf{u}_2]^T = \mathbf{A}[\mathbf{w}_1 \ \mathbf{w}_2]^T$. Since $\mathbf{A}$ is full rank, each possible input $[\mathbf{w}_1 \ \mathbf{w}_2]^T$ is mapped to a unique output $[\mathbf{u}_1 \ \mathbf{u}_2]^T$. From the problem statement, $\mathbf{w}_1$ takes on 2^{nR_1} possible values and $\mathbf{w}_2$ takes on 2^{nR_2} possible values, so the input space contains $2^{n(R_1+R_2)}$ elements.

Next. we consider $|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2)|$. Without loss of generality, assume that $R_1 > R_2$. Then, for each of the 2^{nR_2} possible $\mathbf{w}_2$, there is exactly one $\mathbf{w}_1$ satisfying $a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2 = \mathbf{u}_2$. Thus, there can only be 2^{nR_2} pairs $(\mathbf{w}_1, \mathbf{w}_2)$ and, since the equation for $\mathbf{u}_1$ is linearly independent from that of $\mathbf{u}_2$, plugging these in yields exactly 2^{nR_2} solutions, which corresponds to $2^{nR_{\text{MIN}}}$. The proof for $|\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1)|$ follows in a similar fashion. ■

B. Achievable Rate Region

We now state the achievable rates for the cardinality-based approach.

Theorem 2: **Two message inverse compute-and-forward.** The messages $\mathbf{w}_1$ and $\mathbf{w}_2$ can be recovered from equations $\mathbf{u}_1 = a_{11}\mathbf{w}_1 \oplus a_{12}\mathbf{w}_2$ and $\mathbf{u}_2 = a_{21}\mathbf{w}_1 \oplus a_{22}\mathbf{w}_2$ sent over a Gaussian MAC if

$$\min(R_1, R_2) < \min(C(S_1), C(S_2)) \tag{3}$$
$$R_1 + R_2 < C(S_1 + S_2). \tag{4}$$

Proof: The result can be shown using a combination of the Cardinality Lemma and a binning argument. We give a full proof below for completeness.

Codebook generation and encoding: Generate $2^{nR_{\text{MAX}}}$ codewords of length n, X_1^n i.i.d $\sim \mathcal{N}(0, S_1)$. Similarly, generate $2^{nR_{\text{MAX}}}$ independent codewords X_2^n i.i.d. $\sim \mathcal{N}(0, S_2)$. Note that both codebooks meet the expected power constraint and the codewords are independent across transmitters. The relays are assumed to have successfully decoded $\mathbf{u}_1$ and $\mathbf{u}_2$, which both lie in alphabets of size $2^{nR_{\text{MAX}}}$. These equation values are used as indices for the transmitted codewords $X_1^n(\mathbf{u}_1)$ and $X_2^n(\mathbf{u}_2)$.

Decoding: The destination receives $Y^n = X_1^n(\mathbf{u}_1) + X_2^n(\mathbf{u}_2) + Z^n$ and decodes the pair $(\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2)$ such that $(X_1^n(\hat{\mathbf{u}}_1), X_2^n(\hat{\mathbf{u}}_2), Y^n)$ is jointly typical if such a pair exists and is unique; otherwise, an error is declared. Knowing $(\mathbf{u}_1, \mathbf{u}_2)$, the destination can uniquely determine the messages $(\mathbf{w}_1, \mathbf{w}_2)$ as $\mathbf{A}$ is full rank.

Analysis of the probability of error: By symmetry, the probability of error does not depend on the transmitted pair $(\mathbf{u}_1, \mathbf{u}_2)$. So, without loss of generality, we assume that $(\mathbf{u}_1, \mathbf{u}_2) = (\mathbf{0}, \mathbf{0})$ was transmitted. An error occurs if the x_1^n and x_2^n corresponding to the correct $(\mathbf{u}_1, \mathbf{u}_2)$ are not typical with the received sequence or if for some $(\mathbf{u}_1, \mathbf{u}_2) \neq (\mathbf{0}, \mathbf{0})$ (that is admissible under $\mathbf{A}$), the associated $x_1^n(\mathbf{u}_1), x_2^n(\mathbf{u}_2)$ are jointly typical with the received sequence. Define the events

$$E_{\mathbf{v}_1,\mathbf{v}_2} = \{(X_1^n(\mathbf{v}_1), X_2^n(\mathbf{v}_2), Y^n) \in A_\epsilon^{(n)}\}, \tag{5}$$

where $A_\epsilon^{(n)}$ is the set of all jointly typical sequences. Using the union bound, we can upper bound the probability of error,

$$\begin{aligned} P_e &= \Pr\left(E_{\mathbf{0},\mathbf{0}}^c \cup \bigcup_{(\mathbf{v}_1,\mathbf{v}_2)\neq(\mathbf{0},\mathbf{0})} E_{\mathbf{v}_1,\mathbf{v}_2}\right) \\ &\leq \Pr(E_{\mathbf{0},\mathbf{0}}^c) + \sum_{\mathbf{v}_1 \in \mathcal{M}_{\mathbf{A}}(U_1|\mathbf{0})\setminus\{\mathbf{0}\}} \Pr(E_{\mathbf{v}_1,\mathbf{0}}) \\ &\quad + \sum_{\mathbf{v}_2 \in \mathcal{M}_{\mathbf{A}}(U_2|\mathbf{0})\setminus\{\mathbf{0}\}} \Pr(E_{\mathbf{0},\mathbf{v}_2}) \\ &\quad + \sum_{(\mathbf{v}_1,\mathbf{v}_2)\in \mathcal{M}_{\mathbf{A}}(U_1,U_2), \mathbf{v}_1\neq\mathbf{0}, \mathbf{v}_2\neq\mathbf{0}} \Pr(E_{\mathbf{v}_1,\mathbf{v}_2}). \end{aligned}$$

By the asymptotic equipartition property, $P(E_{\mathbf{0},\mathbf{0}}^c) \to 0$ as $n \to \infty$. Now, for $\mathbf{v}_1 \in \mathcal{M}_{\mathbf{A}}(U_1|\mathbf{0}) \setminus \{\mathbf{0}\}$:

$$\begin{aligned} \Pr(E_{\mathbf{v}_1,\mathbf{0}}) &= P((X_1^n(\mathbf{v}_1), X_2^n(\mathbf{0}), Y^n) \in A_\epsilon^{(n)}) \\ &= \sum_{(x_1^n, x_2^n, y^n)\in A_\epsilon^{(n)}} p(x_1^n)p(x_2^n, y^n) \\ &\leq 2^{-n(H(X_1)+H(X_2,Y)-H(X_1,X_2,Y)-\epsilon)} \\ &= 2^{-n(I(X_1;Y|X_2)-\epsilon)} \end{aligned}$$

Similarly for $\mathbf{v}_2 \in \mathcal{M}_{\mathbf{A}}(U_2|\mathbf{0}) \setminus \{\mathbf{0}\}$:

$$\Pr(E_{\mathbf{0},\mathbf{v}_2}) \leq 2^{-n(I(X_2;Y|X_1)-\epsilon)},$$

and for $(\mathbf{v}_1, \mathbf{v}_2) \in \mathcal{M}_{\mathbf{A}}(\mathbf{u}_1, \mathbf{u}_2), \mathbf{v}_1 \neq \mathbf{0}, \mathbf{v}_2 \neq \mathbf{0}$,

$$P(E_{\mathbf{v}_1,\mathbf{v}_2}) \leq 2^{-n(I(X_1,X_2,Y)-\epsilon)}.$$

Finally, by the Cardinality Lemma,

$$\begin{aligned} P_e \leq \epsilon &+ |\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{0})|2^{-n(I(X_1;Y|X_2)-\epsilon)} \\ &+ |\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{0})|2^{-n(I(X_2;Y|X_1)-\epsilon)} \\ &+ |\mathcal{M}_{\mathbf{A}}(U_1,U_2)|2^{-n(I(X_1,X_2;Y)-\epsilon)} \\ &= \epsilon + 2^{nR_{\text{MIN}}}2^{-n(I(X_1;Y|X_2)-\epsilon)} \\ &\quad + 2^{nR_{\text{MIN}}}2^{-n(I(X_2;Y|X_1)-\epsilon)} \\ &\quad + 2^{n(R_1+R_2)}2^{-n(I(X_1,X_2;Y)-\epsilon)}. \end{aligned}$$

Thus, to ensure $P_e \to 0$ as $n \to \infty$, it is sufficient if

$$\begin{aligned} R_{\text{MIN}} &< I(X_1;Y|X_2) = C(S_1) \\ R_{\text{MIN}} &< I(X_2;Y|X_1) = C(S_2) \\ R_1 + R_2 &< I(X_1, X_2; Y) = C(S_1 + S_2), \end{aligned}$$

where we have evaluated the mutual information terms over the i.i.d. Gaussian input distributions. ∎

Remark: Note that the special case with one zero coefficient results in a slightly different region. Specifically, the size of the sets in the Cardinality Lemma will change, thereby altering the left-hand sides of the achievable rate region of Theorem 2. In particular, if Relay 1 decodes an equation with non-zero coefficients and Relay 2 decodes an equation with $a_{22} \mod \mathbb{F}_p = 0$ then the region will become

$$R_2 < I(X_1;Y|X_2) = C(S_1) \tag{6}$$
$$R_{min} < I(X_2;Y|X_1) = C(S_2) \tag{7}$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2). \tag{8}$$

IV. Approach II: Multiple Access with a Common Message

An alternative approach to this problem is to view the two equations $\mathbf{u}_1$ and $\mathbf{u}_2$ as two private messages and a common message. Assume, without loss of generality, that $R_1 > R_2$. Let $\mathbf{w}_1^P$ denote the first k_2 symbols of $\mathbf{w}_1$ and $\mathbf{w}_1^C$ the remaining $k_1 - k_2$ symbols. Recall that $\mathbf{w}_2$ is zero-padded to length k_1 so that the summations are well-defined.[3]

[3]This zero-padding can also be viewed as the nesting of the lattice used at transmitter 2 in that used at transmitter 1.

Therefore, each relay can determine the length k_2 equation $\mathbf{u}_\ell^P = a_{\ell 1}\mathbf{w}_1^P \oplus a_{\ell 2}\mathbf{w}_2$ and the length $k_1 - k_2$ common message $\mathbf{w}_1^C$ from its equation $\mathbf{u}_\ell = a_{\ell 1}\mathbf{w}_1 \oplus a_{\ell 2}\mathbf{w}_2$. Furthermore, since the equations are assumed to be linearly independent, $\mathbf{u}_1^P$ and $\mathbf{u}_2^P$ are independent and uniform over $\mathbb{F}_p^{k_2}$.

The scenario above is exactly equivalent to a multiple-access channel with a common message. The capacity region of this channel was derived by Slepian and Wolf [21] and we reproduce it below for completeness.

Theorem 3 (Slepian-Wolf): Consider a discrete memoryless MAC $p_{Y|X_1X_2}$. Let w_0 be a common message of rate R_0 available at both transmitters and let w_1, w_2 denote private messages of rates R_1 and R_2 that are available at transmitter 1 and 2, respectively. The capacity region for sending (w_0, w_1, w_2) to the receiver is the convex closure of all rate tuples (R_0, R_1, R_2) satisfying

$$R_1 < I(X_1; Y|X_2, V) \tag{9}$$

$$R_2 < I(X_2; Y|X_1, V) \tag{10}$$

$$R_1 + R_2 < I(X_1, X_2; Y|V) \tag{11}$$

$$R_0 + R_1 + R_2 < I(X_1, X_2; Y) \tag{12}$$

for some $p_V(v)p_{X_1|V}(x_1|v)p_{X_2|V}(x_2|v)$.
This result can be extended to Gaussian multiple-access channels using the usual quantization arguments.

It follows that we can cast the two-user inverse compute-and-forward problem as a multiple-access channel with common messages, for which the capacity is known. Note that this approach improves upon the performance of Theorem 2 as it allows for dependent inputs. However, the cardinality-based approach may prove useful in networks with several destinations, each of which only want a subset of the messages. This is the subject of ongoing work.

V. Beyond two users

For the inverse-compute-and-forward problem with more than two users, a number of concepts generalize in a straightforward manner, but one new concept arises, that of "equation alignment". Assume that there are three relays, each with an equation $\mathbf{u}_\ell = a_{\ell 1}\mathbf{w}_1 \oplus a_{\ell 2}\mathbf{w}_2 \oplus a_{\ell 3}\mathbf{w}_3$ of the messages $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$. Furthermore, assume that the matrix of coefficients $\mathbf{A}$ and all of its submatrices are also full rank. For the sake of succinctness, assume all coefficients are non-zero. In this special case, both the cardinality-based approach and the common message approach generalize naturally.

Let R_{MAX} and R_{MIN} denote the largest and smallest of the message rates R_1, R_2, R_3 and let R_{MID} denote the remaining rate. For the cardinality-based approach, the key issue is determining the cardinality of the sets of allowable equations. Clearly, $|\mathcal{M}_{\mathbf{A}}(U_1, U_2, U_3)| = 2^{n(R_1+R_2+R_3)}$ since $\mathbf{A}$ is full rank. Given one equation, say $\mathbf{u}_3$, we can completely eliminate the highest rate message, say $\mathbf{w}_1$, from both remaining equations $\mathbf{u}_1, \mathbf{u}_2$ to get two new equations that only depend on $\mathbf{w}_2$ and $\mathbf{w}_3$. Thus, $|\mathcal{M}_{\mathbf{A}}(U_1, U_2|\mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_1, U_3|\mathbf{u}_2)| = |\mathcal{M}_{\mathbf{A}}(U_2, U_3|\mathbf{u}_1)| = 2^{n(R_{\text{MID}}+R_{\text{MIN}})}$. Similarly, given two equations, we can eliminate all but the lowest rate message from the remaining equation, which implies that $|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{nR_{\text{MIN}}}$. Combining these bounds with a binning argument will yield an achievable rate region.

Just as in the two-user case, each relay can cast its equation as a collection of independent private messages and common messages shared by a subset of the transmitters. In the three user case, all relays will share a common message of rate $R_{\text{MAX}} - R_{\text{MID}}$. Two will share another common message of rate $R_{\text{MID}} - R_{\text{MIN}}$ and the other will have a private message of the same rate. Finally, all relays will have a private message of rate R_{MIN}. This is a special case of a multiple access channel where each transmitter has a subset of a set of independent messages. The capacity region of this channel was derived by Han [22].

Remark: message and equation alignment. Alignment in the transmitted equations makes the cardinality more difficult to evaluate. Here, alignment means that all the submatrices are not full rank. As a result, different transmitted equations may contain the same sub-equations. For example, consider a 3-user multiple-access channel with equations $\mathbf{u_1} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \mathbf{w}_3$, $\mathbf{u_2} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus 3\mathbf{w}_3$, and $\mathbf{u_3} = \mathbf{w}_1 \oplus 2\mathbf{w}_2 \oplus 3\mathbf{w}_3$. Note that $\mathbf{u_1}$ and $\mathbf{u_2}$ contain the same sub-equation $\mathbf{w}_1 \oplus \mathbf{w}_2$. This means that $|\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{n\min(R_1,R_2)}$ instead of $2^{nR_{\text{MIN}}}$. Thus, alignment makes it more difficult to recover the full set of messages from the equations. More generally, if there are multiple receivers with differing demands, it is possible that alignment could improve the achievable rates.

VI. Case Study

We now consider the model of Fig. 1 and derive an achievable rate region through the combination of the CF and ICF schemes. We compare this example to a channel model in which the interference terms have been removed. We will use the achievable rate region of the cardinality-based scheme to emphasize that the gains are not due the use of dependent inputs distributions on the MAC.

The two-hop relay network in Fig. 1 with has two sources (Nodes 1 and 2), two relays (Nodes 3 and 4) and one destination (Node 5) with respective inputs/outputs X_i and Y_i described by

$$\begin{aligned} Y_3 &= X_1 + X_2 + Z_3, \\ Y_4 &= X_1 - X_2 + Z_4, \\ Y_5 &= X_3 + X_4 + Z_5, \end{aligned}$$

where $E[|X_i|^2] \le S_i$ $(i = 1, 2, 3, 4)$, and Z_3, Z_4 and Z_5 are i.i.d. $\sim \mathcal{N}(0, 1)$. To simplify the description of the CF rates, we assume $S_1 = S_2 = S$.

Using the compute-and-forward scheme of [1], relay node 3 is able to decode $\mathbf{w_1} \oplus \mathbf{w_2}$, and relay node 4 may decode $\mathbf{w_1} \ominus \mathbf{w_2}$ with constraints (13) – (14). On the last link, by Theorem 2, destination node 5 may decode the individual messages $\widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$ as long as (15) and (16) hold. Thus, using time-sharing, the combined CF, ICF region that we achieve is

the convex hull of the intersection of (13) – (16).

$$R_1 < \frac{1}{2}\log\left(\frac{1}{2}+S\right), \tag{13}$$

$$R_2 < \frac{1}{2}\log\left(\frac{1}{2}+S\right), \tag{14}$$

$$\min(R_1,R_2) < \min\left(\frac{1}{2}\log(1+S_3), \frac{1}{2}\log(1+S_4)\right) \tag{15}$$

$$R_1+R_2 < \frac{1}{2}\log(1+S_3+S_4). \tag{16}$$

The CF and ICF rate regions, their intersection, and the convex hull of their intersection are illustrated in Fig. 3.

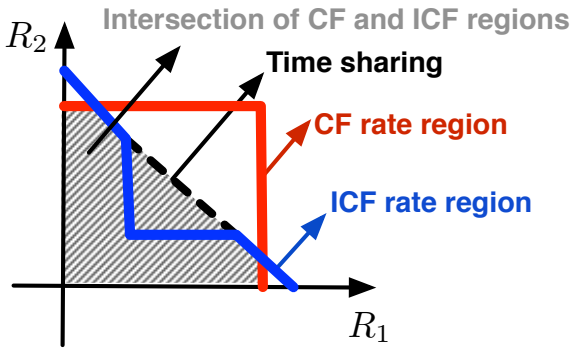

Fig. 3. Convex hull of intersection of CF and ICF rate regions.

When the interfering links between the sources and relays are removed, the capacity of the channel between sources and relays is that of two parallel channels. The second hop from the relays to the destination is a multiple-access channel whose capacity is also known. It can be shown that the capacity region of this network is

$$R_1 < \min\left\{\frac{1}{2}\log(1+S), \frac{1}{2}\log(1+S_3)\right\} \tag{17}$$

$$R_2 < \min\left\{\frac{1}{2}\log(1+S), \frac{1}{2}\log(1+S_4)\right\} \tag{18}$$

$$R_1+R_2 < \frac{1}{2}\log(1+S_3+S_4). \tag{19}$$

At high SNR, the region (14) – (16) strictly contains (17) – (19), emphasizing that we not only mitigate the effect of interference but also exploit it. For example, if $R_1 > R_2$ but $S_3 < S_4$, the network with interfering links can make use of the higher power at Relay 2 to send $\mathbf{w}_1$. If the interfering links are removed, S_3 is a bottleneck on R_1.

VII. Conclusion

In this work, we have studied the inverse compute-and-forward problem, where a receiver wants to recover messages from equations at the relays. The key aspect of this scheme is that the relays do not need to send the equations in their entirety to the receiver. This is due to the fact that knowing one equation restricts the possible values of the other equation if the rates are asymmetric. This problem can also be viewed as a multiple-access channel with a common message. Through a case study, we demonstrated that this strategy, coupled with compute-and-forward, can achieve rate pairs that are outside the rate region of the same network without interference.

Acknowledgements

The work of Y. Song and N. Devroye was partially supported by NSF under award 1053933. The contents of this article are solely the responsibility of the authors and do not necessarily represent the official views of the NSF.

References

[1] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, to appear.

[2] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathsf{SNR})$ on the AWGN channel with lattice encoding and decoding ," *IEEE Trans. Inf. Theory*, 2004.

[3] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[4] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[5] R. Zamir, "Lattices are everywhere," in *ITA*, La Jolla, CA, 2009.

[6] W. Nam, S. Y. Chung, and Y. 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, Nov. 2010.

[7] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[8] D. Gunduz, A. Yener, A. Goldsmith, and H. Poor, "The multi-way relay channel," in *ISIT*, Seoul, Jul. 2009, pp. 339–343.

[9] A. Sezgin, A. Avestimehr, M. Khajehnejad, and B. Hassibi, "Divide-and-conquer: Approaching the capacity of the two-pair bidirectional Gaussian relay network," *Arxiv preprint arXiv:1001.4271*, 2010.

[10] G. Bresler, A. Parekh, and D.N.C. Tse, "The approximate capacity of the many-to-one and one-to-many Gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4566–4592, Nov. 2010.

[11] S. Sridharan, A. Jafarian, S. Vishwanath, S. A. Jafar, and S. Shamai (Shitz), "A layered lattice coding scheme for a class of three user Gaussian interference channels." [Online]. Available: http://arxiv.org/abs/0809.4316

[12] W. Nam, S.-Y. Chung, and Y. Lee, "Nested lattice codes for gaussian relay networks with interference," 2009. [Online]. Available: http://arxiv.org/PS cache/arxiv/pdf/0902/0902.2436v1.pdf

[13] Y. Song and N. Devroye, "List decoding for nested lattices and applications to relay channels," in *Allerton*, Monticello, IL, Sep. 2010.

[14] T. Philosof, R. Zamir, and A. Khisti, "Lattice strategies for the dirty multiple access channel," Submitted to *IEEE Trans. Inf. Theory*, 2009.

[15] D. Krithivasan and S. S. Pradhan, "Lattices for distributed source coding: Jointly Gaussian sources and reconstruction of a linear function," 2009. [Online]. Available: http://arxiv.org/abs/0707.3461

[16] Y. Song and N. Devroye, "Structured interference-mitigation in two-hop networks," in *Information Theory and Applications Workshop*, La Jolla, Feb. 2011.

[17] E. Tuncel, "Slepian-Wolf coding over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, April 2006.

[18] L.-L. Xie, "Network coding and random binning for multi-user channels," in *Canadian Workshop on IT*, Edmonton, Alberta, June 2007.

[19] G. Kramer and S. Shamai, "Capacity for classes of broadcast channels with receiver side information," in *ITW*, Tahoe City, CA, September 2007.

[20] T. J. Oechtering, C. Schnurr, I. Bjelakovic, and H. Boche, "Broadcast capacity region of two-phase bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, January 2008.

[21] D. Slepian and J. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. Journal*, vol. 52, no. 7, pp. 1037–1076, 1973.

[22] T. S. Han, "The capacity region of general multiple-access channel with certain correlated sources," *Inform. Control*, vol. 40, no. 1, 1979.