Cooperative Compute-and-Forward

Matthew Nokleby, Member, IEEE, and Behnaam Aazhang, Fellow, IEEE

Abstract

We propose a class of cooperative transmission schemes for compute-and-forward networks. We devise a lattice-coding approach to superposition block Markov encoding with which we construct a computation coding strategy that leverages decode-and-forward cooperation among transmitters. Transmitters broadcast lattice codewords, decode each other’s messages, and then cooperatively transmit resolution information which aids relays in decoding finite-field linear combinations of the incoming messages. Compared to existing non-cooperative techniques, this approach offers substantial improvement in achievable rate and robustness to variation in channel gains. With these results, we derive new achievability schemes for several wireless topologies, most notably a cooperative multi-way relay channel. We show not only that these schemes achieve near-capacity rates in many regimes, but also that they particularly improve the rates of users with weak channels. In this sense, user cooperation introduces a flavor of diversity advantage into compute-and-forward systems.

I. INTRODUCTION

Interference is the primary obstacle to communications over wireless networks. Due to the broadcast nature of the wireless medium, a transmitter’s signal arrives not only at its intended receiver(s), but also at any terminal in the vicinity. This fact has proven to be a formidable challenge to the analysis and design of wireless networks. Despite decades of study and a plethora of sophisticated techniques, the capacity of even the two-user interference channel remains unknown in general, and many approaches to interference entail the minimization of its
effects. A special case of the Han-Kobayashi scheme [1], in which receivers decode a portion of the interference, was recently shown to achieve rates within one bit of the capacity region of the two-user interference channel [2]. Interference alignment, in which interfering signals are made to lie in a low-dimensional subspace of the signal space, has been shown to provide the optimal degrees of freedom (DoF) of the interference channel [3]–[6]. In each of these strategies, the goal is to minimize the effective interference seen by each receiver.

In recent decades, researchers have also developed techniques that exploit, rather than counteract, the broadcast nature of wireless. One of these techniques is cooperative communications. Having origins in the work of van der Meulen [7] and Cover and El Gamal [8], cooperative communications is founded on the idea that nearby terminals can overhear transmissions and facilitate communications between transmitters and receivers. Cooperative strategies such as decode-and-forward and compress-and-forward improve achievable rates for relay, multiple-access, and interference networks [9]–[12]. For large multicast networks, compress-and-forward and similar relaying strategies achieve rates to within a gap of capacity [13], [14]. Further, cooperation offers a diversity advantage [15]–[19], providing robustness against fading channels similar to that of multiple-antenna systems.

Another technique is compute-and-forward [20], also called physical-layer network coding [21]. In compute-and-forward relays decode finite-field linear combinations of incoming codewords rather than the individual codewords. In [20], the computation capacity—that is, the encoding rate regions for which relays can recover suitable linear combinations—is studied for an interference topology. The achievable encoding rates are realized by lattice coding. Transmitters broadcast lattice codewords, noisy linear combinations of which arrive at the relays, and each relay decodes its incoming signal to an integer combination of the lattice codeword. Relays forward the decoded linear combinations “downstream” in the network, and after obtaining sufficiently many linear combinations destination terminals can recover their intended codewords. For example, [22] shows that compute-and-forward relaying achieves near-capacity performance for a class of multicast networks, and [23], [24] show similar results for multi-way relay channels.

The strategy proposed in [20] requires a correspondence between the channel gains and the
desired integer combinations. If the channels do not induce suitable linear combinations of transmitters’ signals, the relays cannot easily recover integer combinations of the lattice points. In [25] it is shown that, absent channel state information, compute-and-forward achieves no greater than two degrees of freedom, which is far short of the cut-set bound, except over a measure-zero set of channel gains. In [25], techniques from real interference alignment [6] are adapted into a compute-and-forward scheme that achieves full DoFs. A tight characterization of the computation capacity at finite SNR, however, remains elusive.

In this paper, we show that cooperative communications improves performance in compute-and-forward networks. We observe that if transmitters were able to encode their messages jointly, compute-and-forward would reduce to a multiple-antenna broadcast channel, the capacity of which is known [26], which enjoys a diversity advantage, and which imposes no constraints on channel gains. Perfect coordination is of course infeasible, but transmitters can partially coordinate by overhearing each other’s messages and then transmitting jointly. Indeed, we show that, for certain topologies, user cooperation is sufficient to achieve performance near the computation capacity at finite SNR, to ensure robustness to channel variations, and to engender resilience to channel failures similar to a diversity advantage.

In Section II we present the system model. Similar to [20], we consider a simple interference topology, except that we introduce links between transmitters by which they can cooperate. We also present a few preparatory results on lattice codes which we use in the sequel. In Section III we present our main result: a cooperative strategy for compute-and-forward. We develop a lattice-coding version of block Markov encoding by decomposing lattice codebooks into to linearly independent constituent codes. The encoding strategy is decode-and-forward in nature. Transmitters broadcast lattice codewords, after which they decode the codewords of other transmitters. They then broadcast a cooperative message: side information corresponding to the linear combinations desired at the relays. To decode, the relays employ a variant of sliding-window decoding tailored to the lattice codebook decomposition, decoding the side information first and the original lattice codewords second.

The proposed strategy garners a substantial improvement in computation rates for two main
reasons. First, cooperating transmitters decode others’ messages, so they can jointly encode portions of the linear combinations directly. Relays therefore need only to decode portions of the linear combinations from separately-encoded messages, which provides robustness against mismatch between channel gains and the desired linear combinations of messages. Second, user cooperation permits a sort of diversity advantage. When one transmitter has a weak channel with the relay(s), other transmitters can decode the message, encode cooperatively the desired linear combination, and transmit it across their (presumably stronger) channels. Our strategy supposes channel state knowledge at the transmitters, so there is no a diversity advantage in the strict sense, but the computation rates of users with weak channels are substantially higher using cooperative compute-and-forward than using non-cooperative strategies.

Similar to the results of [20], the computation capacity results of Section III are building blocks for signaling strategies for larger networks. In Section IV we apply our results to several “use cases”. We examine both interference topologies and a cooperative multi-way relay channel. In each case, we derive new achievable rate regions which outperform existing techniques. We further show that, in certain regimes, the cooperative schemes achieve rates to within a constant of capacity. Finally, numerical results verify the “diversity” advantage offered by cooperation.

Notation: We use bold uppercase letters (e.g. \( \mathbf{A} \)) to refer to matrices and bold lowercase letters (e.g. \( \mathbf{x} \)) to refer to column vectors. For \( n \times m \) matrix \( \mathbf{A} \), \( \mathbf{a}_i \) refers to the \( i \)th column of \( \mathbf{A} \), i.e. \( \mathbf{A} = [\mathbf{a}_1 \cdots \mathbf{a}_m] \). We denote subvectors of a vector using \( \mathbf{x}[a : b] = (x_a, x_{a+1}, \cdots, x_b)^T \), where \((\cdot)^T\) is the usual transpose. Let \( \|\cdot\| \) denote the Euclidean norm. Let \( \circ \) denote the element-wise or Hadamard product. Let \( \mathbb{R} \) and \( \mathbb{Z} \) denote the fields of reals and integers, respectively. Let \( \mathbb{F}_p \) denote the finite field of characteristic \( p \), let \( \oplus \) denote addition modulo \( p \), and let \( a \ominus b \) be the sum of \( a \) and the additive inverse of \( b \). Let \( [x]^+ = \max\{x, 0\} \) denote the positive part of \( x \).

II. Preliminaries

A. System Model

For most of this paper we consider the channel depicted in Figure I. It consists of \( L \) transmitters and \( M \leq L \) relays communicating over a discrete-time real Gaussian channel. Each of the \( L \)
users has $B$ messages $w_l(b) \in \mathbb{F}_p^{k_l}$, for $1 \leq b \leq B$, with $B, k_l \in \mathbb{Z}$. Structurally, this network resembles the compound multiple-access channel or, when $M = L$, the interference channel. However, unlike those more traditional networks, here each relay intends to decode a finite-field linear combination of the transmitters’ messages:

$$f_m(b) = \bigoplus_{l=1}^{L} a_{ml} w_l(b),$$

(1)

for $a_{ml} \in \mathbb{Z}$, and with each $w_l(b)$ is zero-padded to length $k = \max_l k_l$ if necessary. Let the matrix $A = [a_{ml}] \in \mathbb{Z}^{M \times L}$ describe the functions computed by the relays.

This computation channel is a building block for larger channels in which receivers, after obtaining from the relays sufficiently many linear combinations of transmitters’ messages, recover from them the desired individual messages. For example, in two- and multi-way relay channels, the relay computes and forwards the modulo sum of users’ codewords, from which the users can decode the desired messages. We will consider these and other scenarios in Section IV.

![Diagram](image.png)

Fig. 1. The cooperative computation channel. $L$ users cooperatively transmit to $M$ relays, which decode the desired linear functions.

In the sequel we will employ block Markov encoding, so we divide transmissions into $B + 1$ blocks of $n \in \mathbb{Z}$ channel uses each. At block $b$, each transmitter $l$ broadcasts a signal $x_l(t) \in \mathbb{R}^n$, subject to an average power constraint $1/n \|x_l(b)\|^2 \leq P$ for some $P > 0$. The sum of the transmitters’ signals, scaled by channel coefficients and corrupted by noise, arrives at each relay:

$$y_m(b) = \sum_{l=1}^{L} h_{ml} x_l(b) + n_m(b),$$

(2)

where $h_{ml} \in \mathbb{R}$ is the channel coefficient from transmitter $l$ to relay $m$, and $n(b)$ is a white,
unit-variance Gaussian random vector. Define the $M \times L$ matrix $H = [h_{ml}]$.

Our focus is user cooperation, in which transmitters overhear each other’s signals. Each transmitter $l$ also obtains the noisy superposition of the other transmitters’ signals:

$$z_l(b) = \sum_{l' \neq l}^{L} g_{ll'} x_{l'}(b) + n_l(b),$$  

(3)

where $g_{ll'} \in \mathbb{R}$ is the channel coefficient from transmitter $l'$ to transmitter $l$, and $n_l(b)$ is again white, unit-variance Gaussian. Also define the matrix $G = [g_{ll'}]$ with diagonal elements equal to zero. The choice of zero for the diagonal elements implies full-duplex operation, meaning that transmitters can transmit and receive simultaneously. We further assume that channel matrices $H$ and $G$ are fixed and known globally among the transmitters and relays.

B. Computation Capacity

Our goal is to characterize the computation capacity of the channel. Because the relays recover functions of incoming messages, the computation capacity is defined slightly differently than the usual Shannon capacity. Each transmitter has an encoder $E_l : \mathbb{R}^{k_l \times B} \times \mathbb{R}^{n \times B} \rightarrow \mathbb{R}^{n \times (B+1)}$, which maps the messages $w_l(b)$ and the received signals $z_l(b)$ to codewords $x_l(b)$. The encoder $E_l$ must be causal, employing only signals $z_l(a)$ for $a < b$ in generating $x_l(b)$. As usual, the encoding rate is defined as the logarithm of the cardinality of the message set divided by the number of channel realizations over which the messages are encoded:

$$R_l = \frac{B \log_2(|\mathbb{F}_p|)}{n(B+1)} = \frac{Bk_l \log_2(p)}{n(B+1)} \approx \frac{k_l \log_2(p)}{n},$$  

(4)

where the approximation holds for large $B$.

Each relay has a decoder $D_m : \mathbb{R}^{n \times (B+1)} \rightarrow \mathbb{R}^{k \times B}$, which maps received signals $y_m(b)$ to estimates $\hat{f}_m(b)$. Let the absolute probability of error be the probability that any relay makes an incorrect estimate of any of the desired functions:

$$P_e = \Pr\{\hat{f}_m(b) \neq f_m(b), \text{for any } 1 \leq m \leq M, 1 \leq b \leq B\}. $$  

(5)
A computation rate tuple \((R_1, \cdots, R_L)\) is said to be achievable if for any \(\epsilon > 0\) there exists a sequence of encoders with encoding rate greater than \(R - \epsilon\) and decoders such that \(P_e \to 0\) as \(n \to \infty\). For fixed channel gains \(H, G\), function coefficients \(A\), and transmit power \(P\), let \(R(H, G, A, P)\) denote the set of achievable computation rate tuples.

We impose limitations on the function coefficients \(A\) to avoid choosing a trivial coefficient matrix, such as the all-zero matrix, for which the computation rates are unbounded. Specifically, we require that \(A\) be a member of the following set:

\[
A = \{ A \in \mathbb{Z}^{M \times L} : \text{rank}(A) = M, \ \forall \ m \ \exists \ l \text{ such that } a_{ml} \neq 0 \}. \tag{6}
\]

The first condition ensures that the recovered functions retain as much information as possible about the individual messages; for \(L = M\) it implies that one can recover the individual messages from the recovered functions. The second condition, which is redundant for \(L = M\), ensures that each transmitter is represented in the recovered messages.

Finally, we define the computation capacity as the closure of the union of achievable rate tuples over the set of permissible coefficient matrices:

\[
C(H, G, P) = \text{clos} \left( \bigcup_{A \in \mathcal{A}} R(H, G, A, P) \right). \tag{7}
\]

In their seminal work, Nazer and Gastpar developed a computation coding strategy based on nested lattice codes \([20]\). It achieves rates satisfying the following:

\[
R_l < \min_{m, a_{ml} \neq 0} \left[ \frac{1}{2} \log_2(1 + P \|h_m\|^2) - \frac{1}{2} \log_2(\|a_m\|^2 + P(\|a_m\|^2 \|h_m\|^2 - |a_m^T h_m|^2)) \right]^+. \tag{8}
\]

The first term in (8) corresponds to the power in the received signal, whereas the second term is a penalty determined by the gap in the Cauchy-Schwarz inequality between \(h_m\) and \(a_m\). The closer \(h_m\) and \(a_m\) are to being co-linear, the smaller is the rate penalty. Since the Nazer-Gastpar scheme was designed for a non-cooperative network, the rate does not depend on \(G\); nevertheless, it serves as a lower bound on the cooperative computation capacity.
C. Lattice Codes

Because our approach is based on lattice coding, we briefly review the basics. Formally, a lattice $\Lambda$ is a discrete additive subgroup of $\mathbb{R}^n$, which implies that for any $\lambda_1, \lambda_2 \in \Lambda$ we have $\lambda_1 + \lambda_2 \in \Lambda$ and $\lambda_1 - \lambda_2 \in \Lambda$. Any lattice can be generated by taking integer combinations of (not necessarily unique) basis vectors. Choosing these basis vectors as columns, we form the generator matrix of $\Lambda$, denoted by $B \in \mathbb{R}^{n \times n}$. Then, the lattice can be written as a transformation of the integer lattice, or $\Lambda = B\mathbb{Z}^n$.

Let $Q_\Lambda(x)$ denote the lattice quantizer, which maps any point $x \in \mathbb{R}^n$ to the nearest point in $\Lambda$. The lattice $\Lambda$ induces a partition of $\mathbb{R}^n$ into the Voronoi regions $V(\lambda) = \{x \in \mathbb{R}^n : Q_\Lambda(x) = \lambda\}$, where ties are broken arbitrarily. Let $V = V(0)$ be the fundamental Voronoi region of $\Lambda$. The mod operation with respect to $\Lambda$ returns the quantization error $x \mod \Lambda = x - Q_\Lambda(x)$, which is always a member of $V$.

Lattice codebooks are constructed using nested lattices. A lattice $\Lambda_1$ is said to be nested in $\Lambda_2$ provided $\Lambda_1 \subseteq \Lambda_2$. We employ nested lattices constructed using Construction A [27], which goes as follows. A fine coding lattice $\Lambda_c$ is created from a random linear $n \times k$ code over $\mathbb{F}_p$, which is “lifted” to the unit cube and nested into a coarse shaping lattice $\Lambda_s$, as follows:

$$\Lambda_c = B_s(Z^n + F_c F_p^k),$$

where $F_c \in \mathbb{F}_p^{n \times k}$ is the random linear codebook, and $B_s \in \mathbb{R}^{n \times n}$ is a generator matrix of $\Lambda_s$. The lattice codebook is defined as $C = \Lambda_c \cap V_s$, and it has rate

$$R = \frac{1}{n} \log_2 |C| = \frac{k \log_2(p)}{n}.$$ 

In [28] it is shown that this codebook construction achieves the capacity of the point-to-point AWGN channel when the lattice codewords are dithered before transmission.

The compute-and-forward strategy proposed in [20] depends on the existence of a mapping from finite-field messages $w$ to lattice codewords $\lambda$ that preserves linearity. Let $\phi$ be the following
mapping from $\mathbb{F}_p^k$ to the lattice codebook $\mathcal{C}$:

$$\phi(w) = [B_s p^{-1} F_c w] \mod \Lambda_s.$$  \hspace{1cm} (10)

Then, it is shown that $\phi$ is a bijection satisfying the following for $a, b \in \mathbb{Z}$:

$$\phi(a w_1 \oplus b w_2) = [a \phi(w_1) + b \phi(w_2)] \mod \Lambda_s.$$  \hspace{1cm} (11)

D. Lattice Subspaces

To apply decode-and-forward style cooperation into compute-and-forward networks, we tailor block Markov encoding to lattice codes. Our approach is based in the decomposition of lattice codebooks into lattice subspaces. For a codebook $\mathcal{C} = \Lambda_c \cap \mathcal{V}_s$ generated via Construction A, let $k_r \leq k$, and let $F_r \in \mathbb{F}_p^{n \times k_r}$ denote the matrix composed of the first $k_r$ columns of $F_c$. Similarly, let $k_v = k - k_r$, where we recall that $k = \max_i k_i$, and let $F_v \in \mathbb{F}_p^{n \times k_v}$ denote the matrix of the remaining $k_v$ columns. Then define the resolution lattice $\Lambda_r$ and the vestigial lattice $\Lambda_v$ as

$$\Lambda_r = B_s (\mathbb{Z}^n + p^{-1} F_r \mathbb{F}_p^{k_r}), \quad \Lambda_v = B_s (\mathbb{Z}^n + p^{-1} F_v \mathbb{F}_p^{k_v}).$$  \hspace{1cm} (12)

By construction $\Lambda_c = \Lambda_r + \Lambda_v$ and $\Lambda_s \subset \Lambda_r, \Lambda_v \subset \Lambda_c$. We can define codebooks using the resolution and vestigial codebooks

$$\mathcal{C}_r = \Lambda_r \cap \mathcal{V}_s, \quad \mathcal{C}_v = \Lambda_v \cap \mathcal{V}_s,$$  \hspace{1cm} (13)

having rates

$$R_r = \frac{k_r}{n} \log_2 p, \quad R_v = \frac{k_v}{n} \log_2 p.$$  \hspace{1cm} (14)

By construction $R_r + R_v = R$. Furthermore, for any $0 \leq R_r \leq R$, we can choose $k_r = \left\lfloor \frac{n R_r}{\log_2(p)} \right\rfloor$ to achieve the desired resolution codebook rate. For any message $w \in \mathbb{F}_p^k$, we can define the

---

\footnote{This terminology is intended to convey the fact that this lattice component encodes the “residual” or “leftover” information. We use this less-common synonym in order to minimize notational confusion.}
projection onto the resolution and vestigial codebook as follows:

\[ \phi_r(w) = [B_s p^{-1} F_r w[1 : k_r]] \mod \Lambda_s, \quad \phi_v(w) = [B_s p^{-1} F_v w[k_r + 1 : k]] \mod \Lambda_s. \] (15)

In other words, we take the first \( k_r \) or remaining \( k_v \) elements of the message, respectively, and map them to the lattice codebook. The result is a member of the resolution or vestigial codebook, respectively. Using these projections, we can define a linear decomposition of the lattice codebook, as depicted in Figure 2.

**Lemma 1:** For any \( w \in \mathbb{F}_p^k \),

\[ \phi(w) = [\phi_r(w) + \phi_v(w)] \mod \Lambda_s. \] (16)

**Proof:** This result follows from the fact that \( \phi \) is a linear mapping. By definition,

\[ w = (w^T[1 : k_r] 0_{k_v}^T)^T \oplus (0_{k_r}^T, w^T[k_r + 1 : k])^T, \] (17)

so

\[ \phi(w) = \phi((w^T[1 : k_r] 0_{k_v}^T)^T \oplus (0_{k_r}^T, w^T[k_r + 1 : k])^T) \]

\[ = [\phi((w^T[1 : k_r] 0_{k_v}^T)^T) + \phi((0_{k_r}^T, w^T[k_r + 1 : k])^T)] \mod \Lambda_s^{(n)} \]

\[ = [\phi_r(w) + \phi_v(w)] \mod \Lambda_s^{(n)}, \]

where the last equality follows from the definition of \( F_r \) and \( F_v \); zeroing out the unwanted portions of \( w \) is equivalent to discarding the associated columns of \( F \).

The codeword \( \phi(w) \in \mathcal{C} \) is therefore the sum of two linearly independent lattice points: \( \phi_r(w) \), which we call the resolution information and which encodes the first \( k_r \log_2 p \) bits of the message, and \( \phi_v(w) \), which we call the vestigial information and which encodes the remaining \( k_v \log_2 p \) bits. Furthermore, as illustrated in the following lemma, the decomposition is linear in that the decomposition of sums of lattice points is the same as the sum of the decompositions.
Fig. 2. Lattice subspace decomposition. Each lattice codeword in $C$ is the sum of a point in $C_r$ (left) and a point in $C_v$ (right). The shaded region $V_s$ defines the codebook, whereas the strip-shaped Voronoi regions $V_r$ and $V_v$ define the decoding regions of the resolution and vestigial codebooks, respectively.

**Lemma 2:** For $w_1, w_2 \in \mathbb{R}_p^k$, let $w = w_1 \oplus w_2$. Then

$$\phi_r(w) = [\phi_r(w_1) + \phi_r(w_2)] \mod \Lambda_s^{(n)},$$

and

$$\phi_v(w) = [\phi_v(w_1) + \phi_v(w_2)] \mod \Lambda_s^{(n)}.$$  

**Proof:** This follows directly from the fact that $\phi$ is an isomorphism:

$$\phi_r(w) = \phi_r(w_1 \oplus w_2)$$

$$= \phi(w_1[1 : k_r] \oplus w_2[1 : k_r])$$

$$= [\phi(w_1[1 : k_r]) + \phi(w_2[1 : k_r])] \mod \Lambda_s^{(n)}$$

$$= [\phi_r(w_1) + \phi_r(w_2)] \mod \Lambda_s^{(n)}.$$

A similar argument holds for $\phi_v$.

The preceding decomposition permits a lattice-coding instantiation of block Markov encoding. After the transmission of a lattice codeword, cooperating users can transmit the lower-rate resolution component. The intended receiver first decodes the resolution component and subtracts it from the received signal, and then the relay needs only to decode the vestigial component, which again has lower rate than the full codebook. Although in this paper we apply the technique
to compute-and-forward, it can be applied to a variety of relay systems. For example, a related work [29] presents an innovative lattice list decoding technique to show that lattice codes can achieve the capacity of the physically degraded three-terminal relay channel. Using our technique, it is straightforward to construct an alternative strategy which establishes capacity regions for three-terminal and two-way relay channels [30].

III. Capacity Results

In this section we study the computation capacity region of the network described in Section II. We present an outer bound on the capacity region derived from cut-set arguments. We then present inner bounds on the capacity region, which are achieved by lattice block Markov strategies.

A. Outer Bound

We obtain the outer bound on the computation capacity region by supposing a genie supplies to the relays all messages except for those of a single transmitter. The result is a compound relay channel whose capacity we bound via cut-set arguments.

Theorem 1: For each transmitter $1 \leq l \leq L$, let $S_l = \{1, \ldots, l-1, l+1, \ldots, L\}$ be the set of transmitters other than transmitter $l$. Then, all achievable rate tuples $(R_1, \ldots, R_L)$ satisfy

$$R_l \leq \max_{A \in A, m, a_{ml} \neq 0} \min_{p(x)} \sup_{S \subset S_l} \min_{S_c} I(x_l, x_S; y_m, z_{Sc} | x_{Sc}),$$

where $p(x)$ is any distribution over the transmitted signals $(x_1, \ldots, x_L)^T$ satisfying the input power constraint, where $x_S$ is the vector of those those elements $x_i$ such that $i \in S$, and where other set-valued subscripts are defined similarly. In other words, we maximize over all valid integer combinations and all input distributions, then minimize over all cuts between transmitter $l$ and the relays that decode a combination involving the message of transmitter $l$.

Proof: Choose a transmitter $l$, and suppose that a genie supplies the messages $w_{l'}(b)$ to the relays for every $l' \neq l$. By the crypto lemma [28], each $f_m(b)$ such that $a_{ml} \neq 0$ is statistically independent of the messages $w_{l'}(b)$, so the relays remain equivocal as to the desired functions. The scenario is equivalent to a compound relay channel, with transmitter $l$ acting as the source,
the transmitters $l'$ acting as relays, and each relay $m$ such that $a_{ml} \neq 0$ acting as destinations all needing the messages $w_l(t)$. We bound the capacity of the compound relay channel via cut-set arguments. For any cut $S \in \mathcal{S}_t$, the capacity of the compound relay channel is bounded by

$$C(H, G, P) \leq \sup_{p(x)} \min_{m, a_{ml} \neq 0} I(x_l, x_S; y_m, z_{SC} | x_{SC}) \tag{21}$$

$$\leq \min_{m, a_{ml} \neq 0} \sup_{p(x)} I(x_l, x_S; y_m, z_{SC} | x_{SC}). \tag{22}$$

Minimizing over all transmitters cuts, and maximizing over all $A \in \mathcal{A}$, we obtain the result. ■

B. Inner Bound

We present inner bounds on the computation capacity, each based a different cooperative strategy. In the first strategy, called subset cooperation, a subset of the transmitters decodes all of the messages, encodes resolution information for the relays, and transmits in the next block. This strategy is useful when transmitters have strong channels with each other, but when disadvantaged transmitters have weak channels to the relays. In the second strategy, called cluster cooperation, the set of transmitters is partitioned into clusters. Transmitters decode in-cluster messages and jointly broadcast resolution information to the relays. This strategy is useful when transmitters are physically separated and have strong channels with only a few other transmitters. In Section IV, we use subset cooperation to establish achievable rates for interference channels and cluster cooperation to establish new achievable rates for multi-way relay channels.

Theorem 2: Let $B \subset \{1, \cdots, L\}$, let $\mathcal{O}_l$ be a permutation of $\{1, \cdots, L\} \setminus \{l\}$, and let $v_0, v_1, \cdots, v_M$ be vectors such that

$$\sum_{m=0}^{M} |v_{ml}|^2 \leq 1, \forall l, \quad v_{ml} = 0, \forall l \neq B, m > 0. \tag{23}$$
Next, define
\[
I_{m,r} = P \left( \|h_m \circ v_0\|^2 + \sum_{m' \neq m,0} |h_m^{T}v_{m'}|^2 \right) \tag{24}
\]
\[
I_{m,v} = P \sum_{m' \neq m,0} |h_m^{T}v_{m'}|^2. \tag{25}
\]

Then, a rate tuple is achievable provided
\[
R_l < \min_{\nu \in B \setminus \{l\}} \frac{1}{2} \log_2 \left( 1 + \frac{P(g_{\nu l}v_0)^2}{1 + P(\sum_{\nu' \in S(l) \setminus \{l\}} (g_{\nu' l}v_0)^2)} \right), \tag{26}
\]
and
\[
R_l < \min_{m,n \neq l} \frac{1}{2} \log_2 \left( 1 + \frac{P|h_m^{T}v_m|^2}{1 + I_{m,r}} \right) + \left[ \frac{1}{2} \log_2 \left( 1 + P \|h_m \circ v_0\|^2 + I_{m,v} \right) - \frac{1}{2} \log_2 \left( \|a_m\|^2 (1 + I_{m,v}) + P \left( \|a_m\|^2 \|h_m \circ v_0\|^2 - |a_m^{T} (h_m \circ v_0)|^2 \right) \right) \right]^+. \tag{27}
\]

We call this the subset cooperation rate region.

Next, let \( S_1, \ldots, S_N \) be a partition of \( \{1, \ldots, M\} \), let \( S(l) \) denote the \( S_n \) containing \( l \), and let \( \mathcal{O}_l \) be a permutation of \( S(l) \setminus \{l\} \). Further, let \( v_0, v_1, \ldots, v_M \) be vectors such that
\[
\sum_{m=0}^{M} |v_{ml}|^2 \leq 1, \forall l. \tag{28}
\]

Next, define the matrix \( H' \in \mathbb{R}^{M \times N} \) by
\[
h_{mn}' = \sum_{l \in S_n} v_{ml} h_{ml}. \tag{29}
\]

Let \( I_{m,r} \) and \( I_{m,v} \) be defined as before. Finally, let \( B \in \mathbb{Z}^{M \times N} \) and \( A' \in \mathbb{Z}^{M \times L} \) be matrices such that \( c_m a_{ml} = b_{nn'} a'_{ml} \) for every \( l \in S_n \), and for fixed constants \( c_m \in \mathbb{Z} \). Then, a rate tuple \( (R_1, \ldots, R_L) \) is achievable provided
\[
R_l < \min_{\nu \in S(l) \setminus \{l\}} \frac{1}{2} \log_2 \left( 1 + \frac{P(g_{\nu l}v_0)^2}{1 + P(\sum_{\nu' \in S_l \setminus \{l\}} (g_{\nu' l}v_0)^2) + P(\sum_{\nu' \notin S(l)} g_{\nu' l}^2)} \right), \tag{30}
\]
We call this the cluster cooperation rate region.

**Proof:** We describe the subset cooperation and cluster cooperation schemes and show that they achieve the rate regions claimed. Rather than offer two separate proofs, we describe the schemes in parallel, pointing out the differences between them as we proceed.

**Encoding:** Each transmitter encodes at rate \( R_l = \frac{k_l}{n} \log_2(p) \) via a lattice codebook \( C = \Lambda_c \cap V_s \), created via Construction A as described above with shaping lattice \( \Lambda_s \) having unit average power. The codebook has a maximum rate \( k/n \log_2(p) \), where again recall that \( k = \max_l k_l \). Transmitter \( l \) encodes its messages \( w_l(t) \in \mathbb{P}_p^{k_l} \) by zero-padding them to length \( k \) and mapping the result to the corresponding codeword in \( C \):

\[
\lambda_l(t) = \phi(w_l(t)).
\]  

(32)

This mapping induces a number of sublattices \( \Lambda_l \subset \Lambda_c \) and codebooks \( C_l \). Each lattice \( \Lambda_l \) can be decomposed into resolution and vestigial components \( \Lambda_{lr} \) and \( \Lambda_{lv} \), giving rise to resolution and vestigial codebooks \( C_{rl} \) and \( C_{vl} \) having rates \( R_{lr} = \frac{k_{lr}}{n} \log_2(p) \) and \( R_{lv} = \frac{k_{lv}}{n} \log_2(p) \), respectively, for \( k_{lr} + k_{lv} = k_l \). By Lemma \[\] each lattice codeword can be decomposed by projecting onto the resolution and vestigial codebooks for each transmitter:

\[
\lambda_{lr}(t) = \phi_{lr}(w_l(t)), \quad \lambda_{lv}(t) = \phi_{lv}(w_l(t)).
\]  

(33)

When transmitting the lattice codeword, each user dithers the lattice point over the shaping region. We define the effective codeword

\[
c_l(t) = [\lambda_l(t) + t_l(t)] \mod \Lambda_s,
\]  

(34)
where $t_l(t)$ is drawn randomly and uniformly over $\mathcal{V}_s$, independent for each $1 \leq l \leq L$ and $1 \leq b \leq B$. Each relay $m$ intends to recover the finite-field linear combination $f_m(t) = \bigoplus_{l=1}^{L} a_{ml}w_l(t)$, which corresponds to the lattice point

$$\lambda_m(t) = \phi(f_m(t)) = \left[ \sum_{l=1}^{L} a_{ml} \lambda_l(t) \right] \mod \Lambda_s. \quad (35)$$

As with the individual codewords, we can decompose $\lambda_m(t)$ into resolution and vestigial components:

$$\lambda_{mr}(b) = \phi_{mr}(f_m(b)), \quad \lambda_{mv}(b) = \phi_{mv}(f_m(b)), \quad (36)$$

where the decomposition into resolution and vestigial codebooks uses $k_{mr} = \max_{l, a_{ml} \neq 0} k_{rl}$ and $k_{mv} = k - k_{mr}$.

Cooperating transmitters will send resolution codewords according to the cooperation modality.

- ** Subset cooperation:** In this case, the transmitters in $\mathcal{B}$ cooperatively transmit $\lambda_{mr}(t)$ to each relay, again dithering the lattice point over $\mathcal{V}_s$. The effective codeword is

$$c_{mr}(b) = [\lambda_{mr}(b) + s_{mr}(b)] \mod \Lambda_s, \quad (37)$$

where $s_{mr}(b)$ is a dither drawn uniformly over $\mathcal{V}_s$ and independent for each $m, b$.

- **Cluster cooperation** In this case, each cluster $\mathcal{S}_n$ sends an integer combination of the each member’s resolution lattice. To this end, define the lattice point

$$\lambda_{mn,r}(b) = \left[ \sum_{l \in \mathcal{S}_n} a'_{ml} \lambda_l(b) \right] \mod \Lambda_s, \quad (38)$$

and the dithered codeword

$$c_{mn,r}(b) = [\lambda_{mn,r}(b) + s_{mn,r}(b)] \mod \Lambda_s, \quad (39)$$

for independent, uniformly-distributed dither $s_{mn,r}(b)$. 


Transmitters encode their $B$ messages over $B+1$ blocks. At block $b = 1$, each transmitter sends only its own lattice codeword:

$$x_l(b) = \sqrt{P}v_0l^c_l(b).$$ (40)

For subsequent blocks $2 \leq b \leq B$, transmitters send a superposition of “fresh” information, corresponding to their own message $w_l(t)$, and resolution information, corresponding to the messages sent in the previous time slot. The details depend on the cooperation modality.

- **Subset cooperation**: We suppose that each transmitter $l \in B$ has decoded $\lambda_{l'}(b-1)$ for each $l' \neq l$, from which it can construct every $\lambda_{m,n}(b-1)$. Each transmitter then sends

$$x_l(b) = \begin{cases} \sqrt{P} \left( v_0l^c_l(b) + \sum_{m=1}^{M} v_ml^c_{m,n}(b-1) \right), & \text{for } l \in B \\ \sqrt{P}v_0l^c_l(b), & \text{otherwise} \end{cases}.$$ (41)

- **Cluster cooperation**: We suppose that each transmitter $l \in S(l)$ has decoded each $\lambda_{l'}(b-1)$ for each $l' \in S(l) \setminus \{l\}$, from which it can construct every $\lambda_{m,n}(b-1)$. Each transmitter then sends

$$x_l(b) = \sqrt{P} \left( v_0l^c_l(b) + \sum_{m=1}^{M} v_ml^c_{m,n}(b-1) \right).$$ (42)

Finally, at block $b = B+1$ there is no new fresh information for the transmitters to send, and transmitters send only the resolution information corresponding to block $B$ according to the cooperation modality.

- **Subset cooperation**: The transmitters send

$$x_l(B+1) = \begin{cases} \sqrt{P} \sum_{m=1}^{M} v_ml^c_{m,n}(T), & \text{for } l \in B \\ 0 & \text{otherwise} \end{cases}.$$ (43)

- **Cluster cooperation**: The transmitters send

$$x_l(B+1) = \sqrt{P} \sum_{m=1}^{M} v_ml^c_{mn,r}(B).$$ (44)
Finally, because $\Lambda_s$ has unit second moment, it follows that

$$\frac{1}{n} \|x_t(b)\|^2 \rightarrow P \sum_{m=0}^{M} v^2_{lm} \leq P,$$

with high probability; therefore the transmit signals obey the average power constraint.

**Decoding:** Decoding proceeds in three stages. Transmitters decode the messages necessary for cooperation, relays decode the resolution codewords sent cooperatively, and finally the relays decode the vestigial codewords.

We start with the first stage, which depends crucially on the cooperation modality.

- **Subset cooperation:** Each transmitter receives the superposition of other transmitters’ signals:

$$z_t(b) = \sqrt{P} \left( \sum_{l_t \neq l} g_{l_l}v_0c_l(t) + \sum_{j=1}^{M} \sum_{n=1}^{N} g_{l_j}v_{mlc}c_{mnr}(b-1) \right) + n_t(b). \tag{46}$$

Supposing that each transmitter $l \in B$ has successfully decoded the messages from block $b-1$, it also knows the resolution codewords and can subtract them from $z_t(b)$. The resulting signal is equivalent to that of an $L-1$-user multiple-access channel. In [20] it was shown that dithered lattice codebooks and successive decoding are sufficient to achieve the corner points of the capacity region of the multiple-access channel. Therefore, letting the permutation $O_t$ define the decoding order, transmitter $l$ succeeds in recovering the codewords so long as the rates satisfy (26).

- **Cluster cooperation:** Again each transmitter receives the superposition of other transmitters’ signals, but in this case we group them into in-cluster and out-of-cluster signals:

$$z_t(b) = \sqrt{P} \left( \sum_{l \in S(t) \setminus \{l\}} g_{l_l}v_0c_l(b) + \sum_{m=1}^{M} \sum_{n=1}^{N} g_{l_m}v_{ml}c_{mnr}(b-1) \right) + \sum_{l \in S(l)^C} \sum_{v \in S(l)^C} g_{l_l}x_{l_t} + n_t(b). \tag{47}$$

Supposing successful decoding in previous blocks, transmitter $l$ can subtract out the in-cluster resolution codewords. The result is a $|S(l)|-1$-user multiple-access channel, similar to that arising out of subset cooperation, except that here the out-of-cluster signals are treated merely as interference. Again letting the permutation $O_t$ define the decoding order,
and treating the out-of-cluster interference as noise, transmitter $l$ succeeds in recovering in-cluster codewords so long as the rates satisfy (30).

Next, we turn to the second stage, in which the relays decode the resolution codewords corresponding to the functions they decode. Again, the details depend on the cooperation modality.

- **Subset cooperation:** To obtain the resolution codeword $\lambda_r(b)$, each relay turns to the signal received in block $b + 1$:

$$
y_m(b + 1) = \sqrt{P} \sum_{l=1}^{L} h_{ml} v_{0l} c_l(b + 1) + \sqrt{P} \sum_{m'=1}^{M} \sum_{l \in B} h_{ml} v_{ml'} c_{m'r}(b) + n_m(b + 1). \quad (48)
$$

Each relay decodes the resolution information treating the interference—in this case the fresh information from each transmitter and the resolution information intended for other relays—as noise. Following [28], the relays apply MMSE scaling and subtract off the dither $s_{mr}(b)$ modulo $\Lambda_s$. They decode successfully so long as each $R_{lr}$ is less than the first term of the RHS of (27).

- **Cluster cooperation:** Again each relay turns to the signal received in block $b + 1$, which in this case is

$$
y_m(b + 1) = \sqrt{P} \sum_{l=1}^{L} h_{ml} v_{0l} c_l(b + 1) + \sqrt{P} \sum_{m' \neq m}^{M} \sum_{n=1}^{N} h'_{mn} c_{mn,r}(b) + n_m(b + 1). \quad (49)
$$

Again each relay treats the interference from fresh information and codewords intended for other relays as noise. In this case, instead of decoding a single cooperatively-encoded lattice point, each relay decodes an integer combination of the codewords from each cluster. In particular, each relay decodes the sum

$$
\left[ \sum_{n=1}^{N} b_{mn} \lambda_{mn,r}(b) \right] \mod \Lambda_s = \left[ \sum_{n=1}^{N} \sum_{l \in S_n} b_{mn} a_{ml} \lambda_{lr}(b) \sum \right] \mod \Lambda_s = [c_m \lambda_{mr}(b)] \mod \Lambda_s.
$$

(50)

Invoking the compute-and-forward rate of [20, Theorem 4], taking $b_m$ as the function coefficients, $h'_m$ as the channel coefficients, and treating the interference as noise, relay $m$ successfully decodes $[c_m \lambda_{mr}(b)] \mod \Lambda_s$, from which it can recover $\lambda_{mr}(b)$, so long as each $R_{lr}$ is less than
Finally, we turn to the third stage, in which each relay decodes the vestigial component \( \lambda_{mv}(b) \) from \( y_m(b) \). Supposing that each relay has successfully decoded the resolution information from block \( b - 1 \), it can subtract that portion of the interference. Furthermore, supposing that each relay has successfully recovered \( \lambda_{mr}(b) \), the relay can subtract it modulo \( \Lambda_s \) from \( y'(b) \). The resulting signal is

\[
y'_m(b) = [\alpha_m y_m(b) - \lambda_{mr}(b)] \mod \Lambda_s
\]

where \( n'(b) \) is the effective noise, consisting of resolution information intended for other relays and the thermal noise \( n(b) \), and having average power \( 1 + I_{m,v} \). We can rewrite \( y'_m \) as a noisy linear combination of vestigial lattice points as follows.

\[
y''_m(b) = \left[ \sum_{l=1}^{L} (\alpha_m \sqrt{P_{hlv}} v_{ml} c_l(b) - a_{ml} t_l(b)) - \lambda_{mr}(b) + \alpha_m n'_m(t) \right] \mod \Lambda_s
\]

Each relay decodes \( \lambda_{mv}(b) \) treating the remaining terms as noise. Following the argument in [20, Theorem 4], the relays choose \( \alpha_m \) to minimize the effective noise, and we conclude that \( \lambda_{mv}(b) \) is decoded successfully so long as each \( R_v \) is less than the second term of the RHS of (27) or (31).

Finally, having recovered both the resolution and vestigial components, each relay constructs its estimate of the desired lattice codeword, from which it can recover the desired finite-field message. Recall that \( R_t = R_{vl} + R_{vl} \). Combining the rates, and choosing \( B \) sufficiently large, we obtain the result.
IV. USE CASES

In this section we describe the use of the preceding capacity results to establish new achievable rates in a few specific channels. In all cases, cooperation improves performance over existing strategies. In particular, cooperation substantially improves the rates of users with weak channels to relays and destinations. In some cases, we can further show that our schemes achieve rates to within a constant gap of the end-to-end capacity.

A. Cooperative Two-to-one Channel

First we examine a network resembling a two-to-one channel [31]. As depicted in Figure 3, there are two transmitters, two relays, and noiseless bit pipes connecting the relays to the final destination, which intends to recover the messages of both transmitters. Relay 1 receives a noisy linear combination of both transmitters’ signals, while relay 2 hears only the signal of user 2. This network corresponds, for example, to a cellular uplink in which one mobile user lies near a cell boundary, and in which the base stations transmit to a central receiver via backhaul links.

![Fig. 3. The cooperative many-to-one channel.](image)

Via cut-set arguments, one can show that the capacity region of this channel is no larger than

$$\mathcal{C}^+ = \left\{ (R_1, R_2) : R_1 \leq \frac{1}{2} \log_2(1 + P(g_{21}^2 + h_{11}^2)), R_2 \leq \frac{1}{2} \log_2(1 + P(g_{12}^2 + h_{21}^2 + h_{22}^2)), R_1 + R_2 \leq \frac{1}{2} \log_2(1 + P(h_{11} + h_{12})^2) + \frac{1}{2} \log_2(1 + Ph_{22}^2) \right\}. \quad (56)$$

We can establish a lower bound on the rate via Theorem 2. Suppose $|h_{12}| \leq |h_{11}|$; if not, a similar lower bound results from using slightly different parameters. The transmitters employ
subset decoding with $B = \{1\}$, $v_{01} = h_{12}/h_{11}$, $v_{02} = 1$, and $v_{11} = \sqrt{1 - v_{01}^2}$. Relay 1 decodes the modulo sum corresponding to $a_1 = (1, 1)^T$, and relay 2 decodes only the message of user 2, or $a_2 = (0, 1)^T$. Then, the relays noiselessly forward the functions to the destination. Because $A$ is full rank, the destination can recover both messages.

Invoking Theorem 2, this scheme achieves rates satisfying

$$R_1, R_2 < \frac{1}{2} \log_2 \left(1 + P(h_{11}^2 + h_{12}^2)\right) - \frac{1}{2}$$

$$R_2 < \frac{1}{2} \log_2 \left(1 + P \cdot \min\{h_{22}^2, g_{12}^2\}\right).$$

When $|g_{12}| \geq |h_{22}|$, cooperation achieves a sum rate within one bit of the outer bound. Furthermore, cooperation provides robustness against channel variations. When $|h_{21}|$ is close to zero, there is no interference and each relay easily decodes a single message. When $|h_{21}|$ is close to one, non-cooperative compute-and-forward works well because the channel matrix is approximately co-linear with an integer matrix. For moderate values of $|h_{21}|$, however, the non-cooperative compute-and-forward rate is low, but as long as $|g_{12}|$ is sufficiently high, the cooperative rate is high, because user 1 can decode $w_2(b)$.

In Figure 4 we illustrate these results numerically. For $h_{11} = 1$, $0 \leq h_{12} \leq 1$ and $P = 30$dB, we plot the sum-rate upper bound against the lower bound for several values of $g_{12} = g_{21}$. For comparison, we also plot the rates achieved by the non-cooperative Nazer-Gastpar scheme, with the function coefficients chosen according to the LLL lattice reduction algorithm.

![Figure 4](image)

**Fig. 4.** Achievable rates for the two-to-one interference channel, as a function of $h_{21}$, for several values of $g_{12} = g_{21}$. 
We point out a few features of Figure 4. For moderate values of $h_{12}$, the non-cooperative rate oscillates. This well-known phenomenon is due to the Cauchy-Schwarz penalty associated with channel coefficients that are far away from rational numbers with small denominators. Cooperation achieves near-capacity performance except when $g_{12} = g_{21}$ is low, in which case non-cooperation yields higher rates for values of $h_{12}$ near to low-denominator rationals.

B. Cooperative Interference Channel

Next, we add the cross term between user 1 and relay 2, as depicted in Figure 5. This network corresponds to a cellular scenario in which both mobile users are close to a cell boundary. With the cross-term, it is impossible in general to align the users’ transmissions to both relays simultaneously, so we cannot expect near-optimal performance as we saw in the previous case. However, cooperation still garners an improvement in rate.

In Figure 6 we plot the minimum rate achieved by subset cooperation, as given by Theorem 2 with $L = M = 2$, against the upper bound. Because there are many parameters to optimize over, we detail our choices. First, we manually optimize over the three possible choices of $B$. For each choice of $B$, and for fixed steering vectors $v_0, v_1, v_2$, the function coefficients $A$ are chosen via the LLL algorithm. For fixed $v_0$, the remaining vectors are chosen depending on $B$. For $B = \{1, 2\}$, zero-forcing beamformers are possible, and we choose the zero-forcers that equally divide the transmit power available for cooperation. For $B$ a singleton, we simply split the remaining power at the cooperating transmitter between the two relays. Finally, since the remaining optimization is non-smooth and non-convex, we choose $v_0$ using MATLAB’s `patternsearch` function. These choices are of course suboptimal, but they provide good
performance in practice. By comparison, we again plot the Nazer-Gastpar rate. We let $g_{12} = g_{21} = 2$ and select $h_{ml} = 1$ for except for $h_{12}$, which we let vary. We plot the rates for several values of $P$.

![Graph showing achievable rates for the cooperative interference channel as a function of $h_{12}$ for several values of $P$.](image)

Fig. 6. Achievable rates for the cooperative interference channel, as a function of $h_{12}$, for several values of $P$.

Again cooperative computation outperforms non-cooperation, although here the gap in performance is smaller. The freedom to choose $v_0$ and use the remaining power for cooperative transmission permits us to counteract the oscillations in the non-cooperative rate, in some cases turning “valleys” into peaks. However, we cannot eliminate the Cauchy-Schwarz penalty at both relays simultaneously.

C. Cooperative Multi-way Channel with Out-of-Band Relay

Finally, we examine a multi-way channel comprising four users who exchange messages through a single dedicated relay, as depicted in Figure 7. Users 1 and 2 have messages intended for users 3 and 4, and vice versa. The relay’s transmission is “out of band,” meaning that it arrives at the users orthogonal to other transmissions. Out-of-bound relaying, which has been studied in a variety of contexts [33], [34], permits the simplification of relaying protocols and captures the behavior of heterogeneous nodes. The four users form two clusters, between which there exist links by which the users cooperate. We model the received signals by the following
equations:
\[
y_1(b) = g_{12}x(b) + n_1, y'_1(b) = h_{1r}x(b) + n'_1(b)
\]
\[
y_2(b) = g_{21}x(b) + n_2, y'_2(b) = h_{2r}x(b) + n'_2(b)
\]
\[
y_3(b) = g_{34}x(b) + n_3, y'_3(b) = h_{3r}x(b) + n'_3(b)
\]
\[
y_4(b) = g_{43}x(b) + n_4, y'_4(b) = h_{4r}x(b) + n'_4(b)
\]
\[
y_r(b) = h_{r1}x_1(b) + h_{r2}x_2(b) + h_{r3}x_3(b) + h_{r4}x_4(b) + n_r(b),
\]
where each noise vector has i.i.d. standard Gaussian elements. By cut-set arguments, the capacity region of this channel is contained in the following set:
\[
C^+ = \left\{ (R_1, R_2, R_3, R_4) : R_1 + R_2 \leq \frac{1}{2} \log_2(1 + P(h_{r1} + h_{r2})^2), \frac{1}{2} \log_2(1 + P(h_{3r}^2 + h_{4r}^2)) \right\}
\]
\[
R_3 + R_4 \leq \frac{1}{2} \log_2(1 + P(h_{r3} + h_{r4})^2), \frac{1}{2} \log_2(1 + P(h_{1r}^2 + h_{2r}^2)) \right\}
\]
\[
R_i \leq \frac{1}{2} \log_2(1 + P(h_{ri}^2 + g_{ji}^2)) \right\}
\]

Using our techniques, we derive a lower bound that is within a constant gap of the outer bound in certain regimes. For integer $B/2$, suppose that each user $l$ has messages $u_l(b) \in \mathbb{F}_p^{k_l}$ for $1 \leq b \leq B/2$. Then, select a transformation $T \in \mathbb{F}_p^{k \times k}$, which we suppose is known globally,
such that both $T$ and $T \oplus I$ are invertible. Then, for $1 \leq b \leq B$, define

$$w_l(b) = \begin{cases} u_l(\lfloor b/2 \rfloor), & b \text{ odd} \\ u_l(b/2), & b \text{ even, } l \text{ odd} \\ Tu_l(b/2), & b \text{ even, } l \text{ even} \end{cases}$$

(59)

In other words, users 1 and 3 transmit the same message in two consecutive blocks, whereas users 2 and 4 transmit a message followed by a linear transformation of that same message. Then, using the cluster cooperation from Theorem 2, the users transmit these messages to the relay. In particular, the users choose $S_1 = \{1, 2\}$ and $S_2 = \{3, 4\}$. Supposing without loss of generality that $|h_{r_1}| \geq |h_{r_2}|$ and $|h_{r_3}| \geq |h_{r_4}|$, they choose $v_{01} = h_{r_2}/h_{r_1}$, $v_{03} = h_{r_4}/h_{r_3}$, and $v_{02} = v_{04} = 1$. They choose the remaining coefficients to match the power constraint. At each block $b$, the relay decodes the modulo sum of each message, corresponding to $a = (1, 1, 1, 1)^T$, which it then broadcasts to the users during block $b + 1$. Denote each modulo sum $w(b)$.

In addition to overhearing individual user transmissions, users 2 and 4 can also decode their in-cluster messages from the resolution codewords transmitted by users 1 and 3, respectively. Subtracting out the resolution components of their own messages, they can decode the resolution components of the desired message, after which they can decode the vestigial components. Doing this, they can decode the in-cluster message at the rate of the point-to-point link between the users, even though users 1 and 3 scale down their transmissions by $v_{01}$ and $v_{03}$, respectively.

From the modulo sums $w(b)$, users 1 and 2 can recover the messages $u_1(b)$ and $u_2(b)$, and users 3 and 4 recover the messages $u_1(b)$ and $u_2(b)$. For example, for odd $b$, user 1 first subtracts $u_1(b)$ and $u_2(b)$, which it already knows, from $w(b)$ and $w(b + 1)$. Call the subtracted versions $w'(b)$ and $w'(b + 1)$, respectively. Then, user 1 forms the linear combinations

$$\begin{align*}
(T \oplus I)^{-1}w'(b) \oplus w'(b + 1) &= u_3(b) \\
T^{-1}(w'(b) \oplus u_3(b)) &= u_4(b).
\end{align*}$$

(60) (61)

The remaining users employ a similar process to recover the desired messages.
Invoking Theorem 2 noting that the users needed two blocks to transmit each message, and recalling that good lattice codes achieve the capacity of the AWGN channel, the preceding scheme achieves the following rates:

\[
C^- = \left\{(R_1, R_2, R_3, R_4) : R_i \leq \frac{1}{4} \log_2(1 + P g_{ji}^2) \right. \\
R_i \leq \frac{1}{4} \log_2(1 + P (h_{r1}^2 + h_{r2}^2 + h_{r3}^2 + h_{r4}^2)) - \frac{1}{2} \\
R_i \leq \frac{1}{4} \log_2(1 + \min_i \{h_{ir}^2 \cdot P\}) \right\}.
\]

Comparing \(C^+\) and \(C^-\), we observe that, so long as \(\min_{i,j,k} \vert g_{ij} - h_{rk} \vert\) and \(\min_{i,j} \vert h_{ir} - h_{jr} \vert\) are bounded above by constants, the sum rate achieved by our scheme comes to within a constant of the sum capacity. Furthermore, we observe the expected robustness to channel failures. If any user has a poor direct link to the relay, it can still transmit at high rate so long as it has a good link with its cluster neighbor. However, because the relay transmits its decoded linear combination to the four users simultaneously, a single link failure between relay and user is enough to force all of the rates low. One could envision a computation scheme involving receiver cooperation to mitigate this issue. Such a scheme, however, is beyond the scope of this work.

We illustrate the performance in Figure 8. We suppose that \(h_{r1} = h_{r3} = h_{ir} = 1\), for all \(i\), that \(g_{21} = g_{12} = g_{34} = g_{43} = g\) for variable \(g\), and that \(h_{r2} = h_{r4} = h\) for variable \(h\). As long as \(h\) is not too small relative to \(g\), the achievable rate is close to the upper bound.

![Figure 8](image-url)

Fig. 8. Achievable rates for the cooperative multi-way channel, as a function of \(h_{r2} = h_{r4} = h\), for several values of \(g_{ij} = g\).
V. CONCLUSION

We have studied the impact of user cooperation on compute-and-forward. Constructing a lattice-coding version of block Markov encoding, we presented a strategy that introduces a “decode-and-forward” element into computation coding. Transmitters decode each other’s messages, enabling them to broadcast resolution information cooperatively to the relays. Our strategy achieves higher computation rates than previous approaches, because transmitters can jointly encode part of their messages and garner a beamforming gain. We applied these results to a few end-to-end wireless topologies, deriving new achievable rates. Most notably, in a four-user multi-way channel, we derive rates that are near to capacity and robust to individual link failures.

Finally, we note that our techniques can be applied to other situations in which one needs to merge lattice codes with decode-and-forward style cooperation. The lattice block Markov approach presented herein is rather general; as mentioned earlier, it can be used to achieve the capacity of the physically degraded relay channel or to achieve the decode-and-forward rates of the cooperative multiple-access channel. We therefore expect these techniques to be useful for developing new strategies and establishing new results in areas where lattice codes and cooperation are applied, such as physical-layer security [35]–[39] and interference channels [40]–[42]. For example, our techniques have been applied to the construction of low-complexity, high-performance codes for practical relay channels [30].

REFERENCES


