Relays that Cooperate to Compute

Matthew Nokleby
Rice University
nokleby@rice.edu

Bobak Nazer
Boston University
bobak@bu.edu

Behnaam Aazhang
Rice University
aaz@rice.edu

Natasha Devroye
University of Illinois - Chicago
devroye@uic.edu

***Abstract*—This paper proposes a new coding scheme that combines the advantages of statistical cooperation and algebraic structure. Consider a multiple-access relay channel where two transmitters attempt to send the modulo-sum of their finite field messages to the receiver with the help of the relay. The transmitters use nested lattice codes to ensure that sums of codewords are protected against noise and to preserve the modulo operation of the finite field. We develop a block Markov coding scheme where the relay recovers the real sum of the codewords and retransmits it coherently with the two transmitters.**

I. Introduction

Consider a wireless network comprised of several users that wish to communicate with each other. In certain scenarios, it is beneficial to have some of these users act like relays to help other users recover their desired messages. This strategy is broadly referred to as *physical-layer cooperation* and includes many powerful schemes such as decode-and-forward, compress-and-forward, and amplify-and-forward [1]–[8]. The key feature uniting these schemes is that they exploit statistical dependencies between the observations of the relays and the destinations to increase the achievable rates. More recently, a new family of schemes, dubbed *physical-layer network coding*, has been proposed to harness the interference property of the wireless medium, through the use of codebooks with appropriate algebraic structure (see [9] for a recent survey). For instance, compute-and-forward enables relays to recover equations of the transmitted messages and pass them towards the destinations [10]. Until recently, these two broad strategies have been studied in isolation: existing coding schemes exploit either statistical dependencies or algebraic structure, but not both. In this paper, we develop a form of relay cooperation for compute-and-forward that can simultaneously benefit from statistical cooperation and algebraic structure. The key is that the relay can directly recover the sum of the codewords and retransmit it for a coherent gain at the destination. Recent work has also investigated user cooperation for compute-and-forward [11]. There, each transmitter exploits the full duplex nature of the channel to recover other transmitters' codewords, which it can then send, along with its own codeword, for a coherent gain.

II. Problem Statement

We will develop our scheme in the context of a Gaussian multiple-access relay channel (MARC) where the destination wishes to decode the *modulo-sum* of the users' messages. See Figure 1 for an illustration. For ease of exposition, we only consider real-valued channels and symmetric rates.

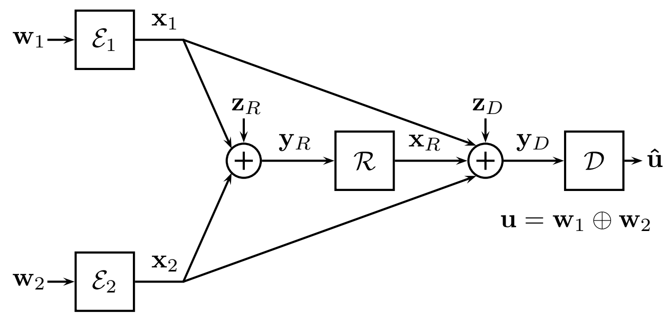

Fig. 1. Compute-and-forward over a Gaussian multiple-access relay channel. The relay helps the receiver decode the modulo-sum of the transmitted messages.

There are two transmitters indexed by $\ell \in \{1, 2\}$, each with a length-k message vector $\mathbf{w}_\ell$, drawn independently and uniformly over a finite field $\mathbb{F}_p^k$, where p is prime. An encoder, $\mathcal{E}_\ell : \mathbb{F}_p^k \to \mathbb{R}^n$, maps this message into a length-n channel input vector $\mathbf{x}_\ell$. As usual, the channel inputs must each satisfy a power constraint, $\|\mathbf{x}_\ell\|^2 \leq nP_S$.

A relay observes the noisy sum of the the channel inputs,

$$\mathbf{y}_R = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z}_R \tag{1}$$

where $\mathbf{z}_R$ is i.i.d. Gaussian noise with mean zero and variance N_R. The relay produces its own channel input $\mathbf{x}_R$ using its causal knowledge of $\mathbf{y}_R$. Specifically, let $\mathcal{R}_i : \mathbb{R}^i \to \mathbb{R}$ denote the mapping that produces the relay's channel input for time i, i.e., the ith component of $\mathbf{x}_R$. The relay's channel input must satisfy a power constraint, $\|\mathbf{x}_R\|^2 \leq nP_R$.

The destination observes the noisy sum of the channel inputs plus the signal from the relay,

$$\mathbf{y}_D = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_R + \mathbf{z}_D \tag{2}$$

where $\mathbf{z}_R$ is i.i.d. Gaussian noise with mean zero and variance N_R. A decoder, $\mathcal{D} : \mathbb{R}^n \to \mathbb{F}_p^k$, produces an estimate $\hat{\mathbf{u}} = \mathcal{D}(\mathbf{y}_D)$ of the modulo-p sum of the messages, $\mathbf{u} = \mathbf{w}_1 \oplus \mathbf{w}_2$.

We say a computation rate R is achievable if, for any $\epsilon > 0$ and n large enough, there exist encoding and decoding functions, such that the relay can reliably decode the sum,

$$\frac{k}{n} \log_2 p > R - \epsilon \tag{3}$$

$$\mathbb{P}(\hat{\mathbf{u}} \neq \mathbf{u}) < \epsilon \ . \tag{4}$$

The computation capacity is the supremum of all achievable computation rates.

III. Nested Lattice Codes

Our achievable scheme relies on the use of nested lattice codes. For completeness, we provide a brief set of definitions below and refer interested readers to [10], [12]–[14] for further details as well as [7], which develops a family of lattice-based decode-and-forward and compress-and-forward schemes for classical relay scenarios. A lattice Λ is a discrete subgroup of $\mathbb{R}^n$ with the property that if $\mathbf{t}_1, \mathbf{t}_2 \in \Lambda$ then $\mathbf{t}_1 + \mathbf{t}_2 \in \Lambda$. Any lattice can be described using a real-valued generator matrix $\mathbf{B} \in \mathbb{R}^n$,

$$\Lambda = \mathbf{B}\mathbb{Z}^n \ . \tag{5}$$

A pair of lattices $\Lambda, \Lambda_{\text{FINE}}$ is nested if $\Lambda \subset \Lambda_{\text{FINE}}$.

With each lattice, we associate a quantizer, $Q_\Lambda : \mathbb{R}^n \to \Lambda$, that maps vectors to the nearest lattice point in Euclidean distance,

$$Q_\Lambda(\mathbf{x}) = \arg\min_{\mathbf{t}\in\Lambda} \|\mathbf{x} - \mathbf{t}\| \ . \tag{6}$$

The fundamental Voronoi region is the subset of points in $\mathbb{R}^n$ that quantize to the zero vector, $\mathcal{V} = \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$. The modulo operation returns the quantization error with respect to the lattice,

$$[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}) \ , \tag{7}$$

and satisfies the distributive law,

$$\big[a[\mathbf{x}] \bmod \Lambda + b[\mathbf{y}] \bmod \Lambda\big] \bmod \Lambda = \big[a\mathbf{x} + b\mathbf{y}\big] \bmod \Lambda \ ,$$

for any integer-valued coefficients $a, b \in \mathbb{Z}$.

A nested lattice code $\mathcal{L}$ is created by taking the set of fine lattice points that fall within the fundamental Voronoi region of the coarse lattice, $\mathcal{L} = \Lambda_{\text{FINE}} \cap \mathcal{V}$. The rate of such a code is $R = \frac{1}{n}\log|\mathcal{L}|$. Erez and Zamir have shown that there exist nested lattice codes that can approach the capacity of a point-to-point Gaussian channel [13]. This capacity-achieving lattice ensemble is created using Construction A, which embeds a finite field codebook into the reals. Specifically, let be the finite field generator matrix for a linear code and $\mathbf{B}$ be the real-valued generator matrix for the coarse lattice Λ. The fine lattice is created as follows:

- Create a finite field generator matrix $\mathbf{G} \in \mathbb{F}_p^{n\times k}$ with every element drawn in an i.i.d. uniform fashion from $\mathbb{F}_p$.
- Let $\mathcal{C}$ denote the codebook induced by $\mathbf{G}$,
$$\mathcal{C} = \{\mathbf{c} = \mathbf{G}\mathbf{w} : \mathbf{w} \in \mathbf{F}_p^k\} \ .$$
- Embed this codebook into the unit cube and tile the result over the integers,
$$\tilde{\Lambda}_{\text{FINE}} = p^{-1}\mathcal{C} + \mathbb{Z} \ .$$
- Rotate by the generator matrix of the coarse lattice to get the desired fine lattice,
$$\Lambda_{\text{FINE}} = \mathbf{B}\tilde{\Lambda}_{\text{FINE}} \ .$$

It can be shown [13], [15] that, for appropriate p and k a lattice drawn from this random ensemble is good for Gaussian channel coding with probability that goes to 1 with n.

For our relaying strategy, we will use a codebook that can be decoded in two stages by the destination. Following the framework set forth in [8], we will split our lattice codebook into two parts, the termed the *resolution codebook* $\mathcal{L}_r$ and *vestigial*[1] *codebook* $\mathcal{L}_v$, respectively. These codebooks are created by splitting the columns of the finite field generator matrix $\mathbf{G} = [\mathbf{G}_r \ \mathbf{G}_v]$ and generating lattices Λ_r and Λ_v from each part following the construction outlined above. In effect, this means that the first k_r symbols of a message are encoded onto Λ_r and the last $k_v = k - k_r$ symbols of a message are encoded onto Λ_v. The rates of $\mathcal{L}_r$ and $\mathcal{L}_v$ are set to R_r and R_v with $R_r + R_v = R$.

As shown in [10, Lemma 6], there exist mappings between finite field vectors and nested lattice codes that preserve linearity. Specifically, there is a one-to-one mapping $\phi : \mathbb{F}_p^k \to \mathcal{L}$ such that for any $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{F}_p^k$,

$$\phi^{-1}\Big([\phi(\mathbf{w}_1) + \phi(\mathbf{w}_2)] \bmod \Lambda\Big) = \mathbf{w}_1 \oplus \mathbf{w}_2 \ . \tag{8}$$

This correspondence can be extended to the resolution and vestigial codebooks [8]. That is, there exist mappings $\phi_r : \mathbb{F}_p^k \to \mathcal{L}_r$ and $\phi_v : \mathbb{F}_p^k \to \mathcal{L}_v$ such that for any $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{F}_p^k$,

$$\phi_r(\mathbf{w}_1 \oplus \mathbf{w}_2) = [\phi_r(\mathbf{w}_1) + \phi_r(\mathbf{w}_2)] \bmod \Lambda \tag{9}$$
$$\phi_v(\mathbf{w}_1 \oplus \mathbf{w}_2) = [\phi_v(\mathbf{w}_1) + \phi_v(\mathbf{w}_2)] \bmod \Lambda \tag{10}$$
$$[\phi_r(\mathbf{w}_\ell) + \phi_v(\mathbf{w}_\ell)] \bmod \Lambda = \phi(\mathbf{w}_\ell) \ . \tag{11}$$

See Lemma 2 and 3 in [8] for a proof.

IV. Compute-and-Forward

Compute-and-forward is a framework for reliably sending linear combinations of finite field messages over multi-user networks [10]. Here, we summarize some of the key results that will be used as building blocks in our scheme.

It was shown in [10] that the computation rate

$$R = \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{P_S}{N_D}\right) \tag{12}$$

is achievable for sending the sum over a two-user multiple-access channel, i.e., the network in Figure 1 with the relay turned off. The basic scheme is described below for completeness.

Encoding: Each user maps its message to a lattice codeword, $\mathbf{t}_\ell = \phi(\mathbf{w}_\ell)$. It then applies a dither[2] that is drawn independently and uniformly over $\mathcal{V}$ and takes $\bmod \Lambda$ to produce its channel input, $\mathbf{x}_\ell = [\mathbf{t}_\ell - \mathbf{d}_\ell] \bmod \Lambda$. The second moment of Λ is chosen to meet the power constraint P_S.

[1] This terminology is intended to convey that the vestigial component of a message is the component "leftover" after the destination has decoded the resolution codeword.

[2] As in the standard random coding argument, these random dithers can be replaced with fixed ones after showing that the scheme works with high probability. That is, no shared randomness is necessary. See [10] for more details.

Decoding: The receiver scales its observation $\mathbf{y}$ by the minimum-mean squared error (MMSE) coefficient $\alpha = \frac{2P_S}{N_D+2P_S}$, removes the dithers, and takes $\bmod \Lambda$ to get

$$\begin{aligned}\mathbf{s} &= \big[\alpha\mathbf{y} - \mathbf{d}_1 - \mathbf{d}_2\big] \bmod \Lambda \\ &= \big[[\mathbf{t}_1 + \mathbf{t}_2] \bmod \Lambda + (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2) + \alpha\mathbf{z}\big] \bmod \Lambda \ .\end{aligned} \tag{13}$$

Thus, the receiver observes the $\bmod \Lambda$ sum of the lattice codewords $\mathbf{v} = [\mathbf{t}_1 + \mathbf{t}_2] \bmod \Lambda$ plus an independent noise term with variance $N_{\text{EFFEC}} = (1-\alpha)^2 2P_S + \alpha^2 N_D = \frac{2P_S N_D}{2P_S+N_D}$. It then quantizes onto the fine lattices and takes $\bmod \Lambda$ to get its estimate of the lattice codeword sum,

$$\hat{\mathbf{v}} = \big[Q_{\Lambda_{\text{FINE}}}(\mathbf{s})\big] \bmod \Lambda \ . \tag{14}$$

Using the results of [13], if

$$R < \frac{1}{2}\log^+\left(\frac{P_S}{N_{\text{EFFEC}}}\right) \ , \tag{15}$$

then, for any $\epsilon > 0$ and n large enough, $\mathbb{P}(\hat{\mathbf{v}} \neq \mathbf{v}) < \epsilon$. Finally, applying the inverse mapping, we obtain a reliable estimate of the modulo-sum of the messages, $\hat{\mathbf{u}} = \phi^{-1}(\hat{\mathbf{v}})$.

Recently, it was shown that if a receiver can recover the $\bmod \Lambda$ sum of the codewords, it can recover the real sum as well [16]. This will be an essential ingredient of our scheme, as it will enable the relay's transmission to coherently combine with those from the source terminals. Below, we state a special case of [16, Lemma 1].

Lemma 1: If a decoder can make an estimate $\hat{\mathbf{v}}$ of $\mathbf{v} = [\mathbf{t}_1 + \mathbf{t}_2] \bmod \Lambda$ with vanishing probability of error, then it can also make an estimate $\hat{\mathbf{q}}$ of the real sum of the channel inputs $\mathbf{q} = \mathbf{x}_1 + \mathbf{x}_2$ with vanishing probability of error.

V. Relay Cooperation for Compute-and-Forward

We now propose a relay cooperation scheme for compute-and-forward. The basic premise is that the relay has a better channel than the destination. To help the destination decode, the relay recovers the real sum of the codewords and retransmits them. To make this work under a causality constraint, we employ block Markov coding in the same fashion as the classical decode-and-forward scheme proposed by Cover and El Gamal [1]. Our main result is a new achievable region for reliable computation over the MARC.

Theorem 1: The computation rate

$$R = \max_{\rho,\gamma\in[0,1]} \max\{R_1(\rho,\gamma), R_2(\rho,\gamma)\} \tag{16}$$

$$\begin{aligned}R_1(\rho,\gamma) = \min\Bigg\{&\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)\gamma^2 P_S}{N_R + (1-\rho^2)(1-\gamma^2)2P_S}\right), \\ &\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{\rho^2 P_S + \frac{P_R}{2} + \rho\sqrt{2P_S P_R}}{(1-\rho^2)2P_S + N_D}\right)\Bigg\} \\ &+ \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)(1-\gamma^2)P_S}{N_D}\right)\end{aligned} \tag{17}$$

$$\begin{aligned}R_2(\rho,\gamma) = \min\Bigg\{&\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)\gamma^2 P_S}{N_R}\right), \\ &\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{\rho^2 P_S + \frac{P_R}{2} + \rho\sqrt{2P_S P_R}}{(1-\rho^2)2P_S + N_D}\right)\Bigg\} \\ + \min\Bigg\{&\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)(1-\gamma^2)P_S}{N_R + (1-\rho^2)\gamma^2 2P_S}\right), \\ &\frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)(1-\gamma^2)P_S}{N_D}\right)\Bigg\}\end{aligned} \tag{18}$$

is achievable for reliably sending the modulo sum of messages over the multiple-access relay channel.

Proof: Using the construction in Section III, we draw a nested lattice codebook $\mathcal{L}$ of rate R and scale it so the second moment of the coarse lattice is equal to P_S. This codebook can be decomposed into resolution and vestigial components, $\mathcal{L}_r$ and $\mathcal{L}_v$, with rates R_r and R_v.

Following standard block Markov encoding, each transmitter encodes B messages $\mathbf{w}_\ell^{[1]}, \ldots, \mathbf{w}_\ell^{[B]}$ each of rate R over $B+1$ blocks of n channel instances each. Assuming correct decoding, this will yield an overall rate of $\frac{B}{B+1}R$, meaning that for large B the rate loss associated with the extra block is negligible. We now describe the encoding and decoding schemes at block 1, block $2 \leq b \leq B$, and block $B+1$. Throughout, it is assumed that the dithers $\mathbf{d}_{\ell,r}^{[b]}$ and $\mathbf{d}_{\ell,v}^{[b]}$ are drawn independently and uniformly over the fundamental Voronoi region of the coarse lattice $\mathcal{V}$ and made available to all terminals. As noted earlier, these random dithers can be replaced with fixed dithers if desired. Let γ and ρ be constants in $[0,1]$ chosen to maximize the rate expression in the theorem statement.

Block 1, Encoding:
Each transmitter maps its message to both the resolution and vestigial lattice codebooks,

$$\mathbf{t}_{\ell,r}^{[1]} = \phi_r(\mathbf{w}_\ell^{[1]}) \qquad \mathbf{t}_{\ell,v}^{[1]} = \phi_v(\mathbf{w}_\ell^{[1]}) \ . \tag{19}$$

It then applies dithers

$$\mathbf{x}_{\ell,r}^{[1]} = [\mathbf{t}_{\ell,r}^{[1]} - \mathbf{d}_{\ell,r}^{[1]}] \bmod \Lambda \qquad \mathbf{x}_{\ell,v}^{[1]} = [\mathbf{t}_{\ell,v}^{[1]} - \mathbf{d}_{\ell,v}^{[1]}] \bmod \Lambda \ .$$

and transmits the weighted sum of these codewords,

$$\mathbf{x}_\ell^{[1]} = \sqrt{1-\rho^2}\Big(\gamma\mathbf{x}_{\ell,r}^{[1]} + \sqrt{1-\gamma^2}\mathbf{x}_{\ell,v}^{[1]}\Big) \ . \tag{20}$$

The relay sends nothing in this block.

Block 1, Decoding: The relay observes

$$\mathbf{y}_R^{[1]} = \sqrt{1-\rho^2}\Big(\gamma\Big(\mathbf{x}_{1,r}^{[1]} + \mathbf{x}_{2,r}^{[1]}\Big) \tag{21}$$

$$+ \ \sqrt{1-\gamma^2}\Big(\mathbf{x}_{1,v}^{[1]} + \mathbf{x}_{2,v}^{[1]}\Big)\Big) + \mathbf{z}_R^{[1]} \ . \tag{22}$$

Since it only needs to recover the sum of the resolution components, it has two options. First, it can decode the resolution sum while treating the vestigial sum as noise. In this case, the effective signal power is $(1-\rho^2)\gamma^2 P_S$ and the effective noise power is $N_R + (1-\rho^2)(1-\gamma^2)2P_S$. Thus, it can recover $\mathbf{x}_{1,r}^{[1]} + \mathbf{x}_{2,r}^{[1]}$ if

$$R_r < \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)\gamma^2 P_S}{N_R + (1-\rho^2)(1-\gamma^2)2P_S}\right) . \tag{23}$$

Second, the relay can initially decode the vestigial sum $\mathbf{x}_{1,v}^{[1]} + \mathbf{x}_{2,v}^{[1]}$, subtract it from the received signal, and then decode the resolution sum without any interference. Using this method, decoding is successful provided

$$R_v < \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)(1-\gamma^2)P_S}{N_R + (1-\rho^2)\gamma^2 2P_S}\right) \tag{24}$$

$$R_r < \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)\gamma^2 P_S}{N_R}\right) . \tag{25}$$

The destination does not recover anything yet.

Block $2 \leq b \leq B$, Encoding:
Each transmitter maps its message to both the resolution and vestigial lattice codebooks,

$$\mathbf{t}_{\ell,r}^{[b]} = \phi_r(\mathbf{w}_\ell^{[b]}) \qquad\qquad \mathbf{t}_{\ell,v}^{[1]} = \phi_v(\mathbf{w}_\ell^{[b]}) \ . \tag{26}$$

It then applies dithers

$$\mathbf{x}_{\ell,r}^{[b]} = [\mathbf{t}_{\ell,r}^{[b]} - \mathbf{d}_{\ell,r}^{[b]}] \bmod \Lambda \qquad \mathbf{x}_{\ell,v}^{[b]} = [\mathbf{t}_{\ell,v}^{[b]} - \mathbf{d}_{\ell,v}^{[b]}] \bmod \Lambda \ .$$

and transmits the weighted sum of these codewords plus the resolution codeword from the previous block,

$$\mathbf{x}_\ell^{[b]} = \sqrt{1-\rho^2}\Big(\gamma\mathbf{x}_{\ell,r}^{[b]} + \sqrt{1-\gamma^2}\mathbf{x}_{\ell,v}^{[b]}\Big) + \rho\mathbf{x}_{\ell,r}^{[b-1]} \tag{27}$$

The relay sends the sum of the resolution codewords from the previous block, scaled to meet its power constraint,

$$\mathbf{x}_R^{[b]} = \sqrt{\frac{P_R}{2P_S}}\Big(\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}\Big) \ . \tag{28}$$

Block $2 \leq b \leq B$, Decoding:
The relay observes

$$\mathbf{y}_R^{[b]} = \sqrt{1-\rho^2}\Big(\gamma\Big(\mathbf{x}_{1,r}^{[b]} + \mathbf{x}_{2,r}^{[b]}\Big) + \sqrt{1-\gamma^2}\Big(\mathbf{x}_{1,v}^{[b]} + \mathbf{x}_{2,v}^{[b]}\Big)\Big)$$

$$+ \ \rho\Big(\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}\Big) + \mathbf{z}_R^{[b]} \ . \tag{29}$$

Since it already know the resolution sum $\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}$ from the previous block, it can remove it and decode the new resolution sum $\mathbf{x}_{1,r}^{[b]} + \mathbf{x}_{2,r}^{[b]}$ using the scheme from block 1.

The destination observes

$$\mathbf{y}_D^{[b]} = \sqrt{1-\rho^2}\Big(\gamma\Big(\mathbf{x}_{1,r}^{[b]} + \mathbf{x}_{2,r}^{[b]}\Big) + \sqrt{1-\gamma^2}\Big(\mathbf{x}_{1,v}^{[b]} + \mathbf{x}_{2,v}^{[b]}\Big)\Big)$$

$$+ \ \left(\rho + \sqrt{\frac{P_R}{2P_S}}\right)\Big(\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}\Big) + \mathbf{z}_D^{[b]} \ . \tag{30}$$

It first decodes the resolution sum $\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}$ from $\mathbf{y}_D^{[b]}$ which is possible if

$$R_r < \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{\rho^2 P_S + \frac{P_R}{2} + \rho\sqrt{2P_S P_R}}{(1-\rho^2)2P_S + N_D}\right) . \tag{31}$$

Assuming the destination decodes correctly, it subtracts the resolution sum from its observation to get $\tilde{\mathbf{y}}_D^{[b]} = \mathbf{y}_D^{[b]} - (\rho + \sqrt{\frac{P_R}{2P_S}})(\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]})$. Next, it takes $\tilde{\mathbf{y}}_D^{[b-1]}$ from the previous block and removes the resolution sum to get

$$\tilde{\mathbf{y}}_D^{[b-1]} - \gamma\sqrt{1-\rho^2}\Big(\mathbf{x}_{1,r}^{[b-1]} + \mathbf{x}_{2,r}^{[b-1]}\Big) \tag{32}$$

$$= \sqrt{1-\rho^2}\sqrt{1-\gamma^2}\Big(\mathbf{x}_{1,v}^{[b-1]} + \mathbf{x}_{2,v}^{[b-1]}\Big) + \mathbf{z}_D^{[b-1]} \ . \tag{33}$$

From here, it can subtract the vestigial sum $\mathbf{x}_{1,v}^{[b-1]} + \mathbf{x}_{2,v}^{[b-1]}$ if

$$R_v < \frac{1}{2}\log^+\left(\frac{1}{2} + \frac{(1-\rho^2)(1-\gamma^2)P_S}{N_D}\right) . \tag{34}$$

Block $B+1$, Encoding:
In the final block, the transmitters and relay coherently send the sum of the resolution codewords from block B,

$$\mathbf{x}_\ell^{[B+1]} = \rho\mathbf{x}_{\ell,r}^{[B]} \tag{35}$$

$$\mathbf{x}_R^{[B+1]} = \sqrt{\frac{P_R}{2P_S}}\Big(\mathbf{x}_{1,r}^{[B]} + \mathbf{x}_{2,r}^{[B]}\Big) \ . \tag{36}$$

Block $B+1$, Decoding:
The relay has nothing to decode in this block. The destination can recover $\mathbf{x}_{1,r}^{[B]} + \mathbf{x}_{2,r}^{[B]}$ from its observation under the same condition as in blocks 2 through B. It then subtracts this resolution sum from $\tilde{\mathbf{y}}_D^{[B]}$ to expose the last vestigial sum, $\mathbf{x}_{1,v}^{[B]} + \mathbf{x}_{2,v}^{[B]}$. Finally, it can recover this sum under the same condition as in blocks 2 through B. The destination now has all of the desired $\bmod \Lambda$ sums of lattice codewords (as well as their real sums). It applies the inverse mapping ϕ^{-1} to each $\bmod \Lambda$ sum to reliably recover its desired message sums, $\mathbf{w}_1^{[1]} \oplus \mathbf{w}_2^{[1]}, \ldots, \mathbf{w}_1^{[B]} \oplus \mathbf{w}_2^{[B]}$. Following standard union bound arguments, it can be shown that the average probability of error goes to zero as n increases. Therefore, there must exist a sequence of good fixed lattice codebooks that achieve the desired rates. ■

Remark 1: In the classical decode-and-forward scheme [1], there is no need to split power between the resolution and vestigial messages. In fact, when the destination turns to decode the vestigial message, it can completely remove the effect of the resolution codeword and obtain the full SNR of the resulting channel to itself. In our considerations, it is not clear how to enable the relay to decode the real sum of the resolution codewords from the real sum of the resolution and vestigial codewords. To overcome this issue, we have split power between the two messages, which results in a small rate loss. Future work will focus on mitigating this effect.

In Figure 2 we plot the achievable rate from Theorem 1. We compare against two similar schemes. First, we compare against the basic compute-and-forward scheme from [10], i.e., the relay is turned off. Second, we compare against a scheme presented in [7] in which the destination decodes the messages individually with the help of the relay. We choose $P_S = 10\text{dB}$, $P_R = 20\text{dB}$, $N_D = 0\text{dB}$, and we vary N_R in order to sweep out a range of values for the signal-to-noise ratio between the transmitters and the relay.

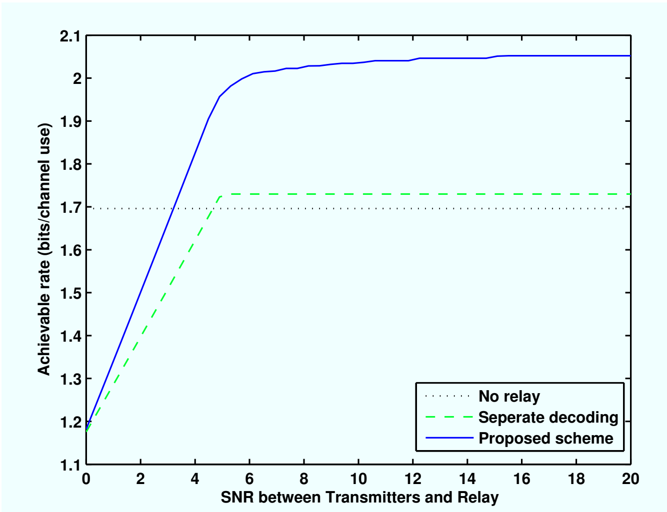

Fig. 2. Achievable rates vs. SNR

For low SNR values, the requirement that the relay must decode the sum constrains the achievable rate, and the basic compute-and-forward scheme dominates. For higher SNR values, the relay can more easily decode, and cooperation nets a rate gain. Both separate decoding and our proposed approach outperform non-cooperation. However, since our approach garners a coherence gain, and since the destination need only decode the sum of messages rather than the messages individually, it outperforms separate decoding for the parameter values shown.

References

[1] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, September 1979.

[2] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3037–3063, September 2005.

[3] B. Schein and R. G. Gallager, "The Gaussian parallel relay network," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2000)*, Sorrento, Italy, June 2000.

[4] S. Borade, L. Zheng, and R. Gallager, "Amplify-and-forward in wireless relay networks: Rate, diversity, and network size," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3302–3318, October 2007.

[5] I. Maric, A. Goldsmith, and M. Médard, "Analog network coding in the high-SNR regime," in *Proceedings of the IEEE Wireless Network Coding Conference (WiNC 2010)*, Boston, MA, June 2010.

[6] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Noisy network coding," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3132–3152, May 2011.

[7] Y. Song and N. Devroye, "Lattice codes for the Gaussian relay channel: Decode-and-forward and compress-and-forward," *IEEE Transactions on Information Theory*, Submitted October 2011, available online: http://arxiv.org/abs/1111.0084.

[8] M. Nokleby and B. Aazhang, "Lattice coding over the relay channel," in *Proceedings of the IEEE International Conference on Communications (ICC 2011)*, Kyoto, Japan, June 2011.

[9] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the* IEEE, vol. 99, no. 3, pp. 438–460, March 2011.

[10] ——, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, October 2011.

[11] M. Nokleby and B. Aazhang, "Cooperative compute-and-forward," *IEEE Transactions on Information Theory*, Submitted March 2012, available online: http://arxiv.org/abs/1203.0695.

[12] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1250–1276, June 2002.

[13] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, October 2004.

[14] R. Zamir, "Lattices are everywhere," in *Proceedings of the 4th Annual Workshop on Information Theory and its Applications (ITA 2009)*, La Jolla, CA, February 2009.

[15] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3401–3416, October 2005.

[16] B. Nazer, "Successive compute-and-forward," in *Proceedings of the International Zurich Seminar on Communications (IZS 2012)*, Zurich, Switzerland, March 2012.