

# Compute-and-Forward: A Novel Strategy for Cooperative Networks

Bobak Nazer and Michael Gastpar  
 University of California, Berkeley  
 Wireless Foundations Center, Department of EECS  
 Berkeley, CA 94720-1770, USA  
 Email: {bobak, gastpar}@eecs.berkeley.edu

**Abstract**—In recent work, we have shown that in a Gaussian network, nodes can often recover linear combinations of transmitted codewords much more efficiently than the codewords themselves. These nodes, after decoding their linear equations, simply send them towards the destination, which given enough equations, can recover the desired messages. This compute-and-forward strategy relies on a lattice-based coding framework. In this note, we show that by employing appropriately nested lattice codes, nodes can reliably recover linear combinations of the messages symbols themselves. This considerably simplifies the description of our scheme. We also consider superposition and successive cancellation within the compute-and-forward framework.

## I. INTRODUCTION

Cooperative communication schemes increase rates in wireless networks by having nodes help other nodes achieve their objectives. In many cases, these cooperative strategies rely on the fact that nodes see linear combinations of neighbors' transmissions. In certain applications, such as distributed MIMO and wireless network coding, it may be useful for a node to forward the observed linear combination of transmissions to other nodes rather than decode the transmissions in their entirety. However, there are many advantages to decoding such as preventing noise from building up inside the network.

In previous work, we have developed a communication strategy, compute-and-forward, that allows intermediate nodes to both recover linear combinations of codewords and eliminate noise [1]. This reduces a network into a set of reliable linear equations (instead of a set of reliable bit pipes). The key to this construction was the use of *lattice codes*. In this note, we present a new construction based on nested lattices that allows nodes to directly recover equations of message symbols over a prime-sized field.

Lattice codes were originally studied to enable practical code constructions to better approach capacity. In [2], Erez and Zamir showed that lattice encoding and decoding are sufficient to approach the capacity of the AWGN channel. Zamir, Shamai, and Erez also showed how to use nested lattices for multiterminal binning in [3]. It has recently been shown that lattice codes (and algebraically structured codes in general) can also serve as a powerful tool for proving new network capacity theorems [4]. This was first noticed by Körner and Marton for the distributed compression of the parity of two correlated binary sources [5]. More recently we

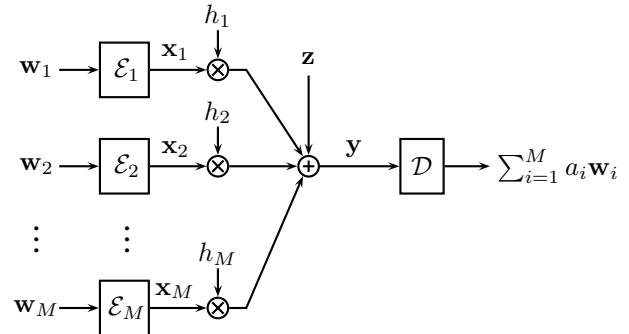


Fig. 1. Reliably decoding an integer combination of the transmitted messages.

have used this phenomenon, which we term *structural gain*, for network coding on the physical layer [6] and reliable computation over multiple-access channels [7]. Others have employed structured codes for combating interference [8]–[10] as well as communicating over the two-way relay channel [11] and distributed Gaussian functional source coding [12].

In this paper, we develop our new coding strategy and characterize the achievable rates. First, we provide some necessary background on lattices and develop our nested lattice construction. Next, we will determine the rate achievable by a single receiver that observes a noisy linear combination for decoding a single equation. Next, we extend this result to the multiple receiver case. Finally, we generalize our scheme to include both superposition and successive cancellation to allow receivers to decode message equations at different rates.

## II. PROBLEM STATEMENT

Our strategy is applicable to any configuration of nodes that communicate through Gaussian channels. We will focus on how to deliver equations across a single cut of the network. We will then show how a destination, given sufficiently many equations, can recover the intended messages. These two components are sufficient to completely describe an achievable rate region for any network.

Consider any cut across a Gaussian network. On one side there are  $L$  transmitters with channel encoders  $\mathcal{E}_1, \dots, \mathcal{E}_L$  and on the other side there are  $M$  receivers with channel decoders  $\mathcal{D}_1, \dots, \mathcal{D}_M$ . We assume that there are different message levels numbered 1 to  $B$ . These will be used for superposition coding of message equations. Each encoder participates in a

subset of message levels which we denote by  $\mathcal{I}_\ell^\varepsilon$ . We assume that our channel encoders take message symbols over the set  $\mathbb{F}_p + j\mathbb{F}_p$  where  $\mathbb{F}_p$  is a prime-sized field and output complex-valued channel inputs:

$$\mathcal{E}_\ell : \{\mathbb{F}_p + j\mathbb{F}_p\}^{\sum_{i \in \mathcal{I}_\ell^\varepsilon} k_i} \rightarrow \mathbb{C}^n \quad (1)$$

where  $k_i$  is the length of the message vector for the  $i^{\text{th}}$  message level and  $n$  is the length of the channel input. We use  $\oplus$  to denote complex addition modulo- $p$  (separately on the real and imaginary parts) and  $+$  to denote regular complex addition,  $\bigoplus_{i \in \mathcal{I}}$  to denote summation modulo- $p$  over the index set  $\mathcal{I}$ , and  $\sum_{i \in \mathcal{I}}$  to denote regular complex summation over the index set  $\mathcal{I}$ . Each decoder participates in its own subset of message levels  $\mathcal{I}_m^D$  and outputs a linear combination of transmitted messages for each message level:

$$\mathcal{D}_m : \mathbb{C}^n \rightarrow \{\mathbb{F}_p + j\mathbb{F}_p\}^{\sum_{i \in \mathcal{I}_m^D} k_i}. \quad (2)$$

We let  $\mathbf{w}_{\ell,b}$  denote the message vector at level  $b$  for encoder  $\ell$ . We say that a decoder recovers the *message equation* from level  $b$  at rate  $R$  if it outputs  $\bigoplus_{\ell=1}^L q_{m\ell,b} \mathbf{w}_{\ell,b}$  and  $k_b n^{-1} 2 \log_2 p = R$ . Let  $\mathbf{q}_{m,b} = [q_{m1,b} \cdots q_{mL,b}]^T$  denote the vector equation coefficients for receiver  $m$  at level  $b$ . Note that these coefficients take values in  $\mathbb{F}_p + j\mathbb{F}_p$ .

Each encoder generates a channel input  $\mathbf{x}_\ell \in \mathbb{C}^n$  that satisfies the power constraint  $\frac{1}{n} E[|\mathbf{x}_\ell|^2] \leq \text{SNR}$ . Each decoder observes a channel output that is a linear combination of the channel inputs plus circularly symmetric Gaussian noise:

$$\mathbf{y}_m = \sum_{\ell=1}^L h_{m\ell} \mathbf{x}_\ell + \mathbf{z}_m \quad (3)$$

where  $h_{m\ell} \in \mathbb{C}$  are the channel coefficients which are fixed for the whole transmission. Let  $\mathbf{h}_m = [h_{m1} \cdots h_{mL}]^T$  denote the vector of channel coefficients to receiver  $m$ . Note that different transmit SNR constraints can be modeled by adjusting the channel coefficients.

In general, each node in a network will have its own message symbols to transmit and will want some subset of the original messages. To this aim, it will recover equations of other users' messages. Some of these equations will be retransmitted into the network and others will be used to recover the desired messages. As usual, we say that node  $\ell$  can achieve a rate  $R$  to node  $m$  if node  $m$  can make an estimate of a message  $\hat{\mathbf{w}}_{\ell,b}$  for some  $b$  such that for any  $\varepsilon > 0$  and  $n$  large enough:

$$\frac{2k_b}{n} \log_2 p > R - \varepsilon, \quad (4)$$

$$\Pr(\hat{\mathbf{w}}_{\ell,b} \neq \mathbf{w}_{\ell,b}) < \varepsilon. \quad (5)$$

Clearly, the general Gaussian network communication problem is extremely difficult, as even the wireline case with a general message structure is unsolved. However, our scheme offers a strict improvement over the standard strategies of successive cancellation and superposition as these are included as special cases. Our coding scheme is based upon a nested lattice construction. The next subsection provides the necessary definitions for lattices.

### A. Nested Lattices

We now reproduce some appropriate definitions from [2]. Note that lattices are defined over the reals.

*Definition 1:* An  $n$ -dimensional *lattice*,  $\Lambda$ , is a set of points in  $\mathbb{R}^n$  such that if  $\mathbf{x}, \mathbf{y} \in \Lambda$ , then  $\mathbf{x} + \mathbf{y} \in \Lambda$ , and if  $\mathbf{x} \in \Lambda$ , then  $-\mathbf{x} \in \Lambda$ . A lattice can always be written in terms of a lattice generator matrix  $\mathbf{L} \in \mathbb{R}^{n \times n}$ :

$$\Lambda = \{\mathbf{x} = \mathbf{w}\mathbf{L} : \mathbf{w} \in \mathbb{Z}^n\}, \quad (6)$$

where  $\mathbb{Z}$  represents the integers.

A pair of lattices  $\Lambda, \Lambda_1$  is said to be nested if  $\Lambda \subset \Lambda_1$ .

*Definition 2:* A *lattice quantizer* is a map,  $Q : \mathbb{R}^n \rightarrow \Lambda$ , that sends a point,  $\mathbf{x}$ , to the nearest lattice point in Euclidean distance:

$$Q(\mathbf{x}) = \arg \min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|_2. \quad (7)$$

*Definition 3:* Let  $[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q(\mathbf{x})$ . For all  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ , the mod  $\Lambda$  operation satisfies:

$$[[\mathbf{x}] \bmod \Lambda + \mathbf{y}] \bmod \Lambda = [\mathbf{x} + \mathbf{y}] \bmod \Lambda \quad (8)$$

$$[q[\mathbf{x}] \bmod \Lambda] \bmod \Lambda = [q\mathbf{x}] \bmod \Lambda \quad \forall q \in \mathbb{Z} \quad (9)$$

*Definition 4:* The *fundamental Voronoi region*,  $\mathcal{V}$ , of a lattice, is the set of all points that are closest to the zero vector:  $\mathcal{V} = \{\mathbf{x} : Q(\mathbf{x}) = \mathbf{0}\}$ . Let  $\text{Vol}(\mathcal{V})$  denote the volume of  $\mathcal{V}$ .

In the next section, we show how to construct good nested lattices.

## III. LATTICE CONSTRUCTIONS

Our main tool for our lattice constructions will be Construction A [13].

Construction A consists of the following steps:

- 1) Given a generator matrix  $\mathbf{G} \in \mathbb{Z}_p^{k \times n}$ , define the codebook  $\mathcal{C}$  as follows:

$$\mathcal{C} = \{\mathbf{c} = \mathbf{w}\mathbf{G} : \mathbf{w} \in \mathbb{Z}_p^k\}. \quad (10)$$

All operations in this step are over  $\mathbb{F}_p$ .

- 2) Form the lattice  $\Lambda$  by tiling the codebook, scaled down by a factor of  $p$ , over  $\mathbb{R}^n$ :

$$\Lambda = p^{-1} \mathcal{C} + \mathbb{Z}^n \quad (11)$$

We will choose the generator matrices for Construction A randomly. This will result in a random ensemble of lattices, which, with high probability, have the desired properties.

For each level  $b = 1, 2, \dots, B$  let  $\mathbf{G}_b$  be a  $k_b \times n$  matrix whose elements are drawn i.i.d. and uniformly over  $\{0, 1, \dots, p-1\}$ . Denote the lattice resulting from Construction A applied to  $\mathbf{G}_b$  as  $\tilde{\Lambda}_b$ . Note that the integer lattice  $\mathbb{Z}^n$  is nested in each  $\tilde{\Lambda}_b$ .

Following the steps in [13], it follows that each  $\mathbf{G}_b$  is full rank with high probability as  $n$  increases.

Erez, Litsyn, and Zamir proved that there exist lattices which are simultaneously good for covering (Rogers goodness) and for channel coding (Polytyrev goodness) [13]. In the interest of space, we simply assume the existence of such a lattice  $\Lambda$  scaled to have second moment  $\frac{\text{SNR}}{2}$  and its corresponding lattice generator matrix  $\mathbf{L} \in \mathbb{R}^{n \times n}$ . We will refer to this lattice

as the *coarse lattice*. Furthermore, we note that this lattice comes from Construction A as well.

Finally, we generate our nested lattice pairs by applying the lattice generator  $\mathbf{L}$  to each  $\tilde{\Lambda}_b$ . We get new fine lattices  $\Lambda_b = \tilde{\Lambda}_b \mathbf{L}$  such that  $\Lambda \subset \Lambda_b$  since the integer lattice is transformed by  $\mathbf{L}$  into  $\Lambda$ . Note that this is the same construction employed by Erez and Zamir in [2] except that here we have multiple fine lattices at different rates.

Note that if  $\mathbf{G}_b$  has rank  $k_b$  (full rank), then the number of fine lattice points in the fundamental Voronoi region of the coarse lattice,  $\mathcal{V}$ , is given by  $|\Lambda_b \cap \mathcal{V}| = p^{k_b}$  so that the rate of  $\Lambda_b$  is  $R_b = \frac{k_b}{n} \log_2 p$ . Furthermore, each message vector  $\mathbf{w} \in \mathbb{F}_p^{k_b}$  is in one-to-one correspondence with a point in  $|\Lambda_b \cap \mathcal{V}|$ .

#### IV. SINGLE RECEIVER COMPUTE-AND-FORWARD

We now focus on the achievable rate for decoding an equation at a single receiver. Furthermore, we limit ourselves to a single message level for now ( $B = 1$ ). Each encoder chooses a message vector  $\mathbf{w}_\ell$  randomly and uniformly from  $\{\mathbb{F}_p + j\mathbb{F}_p\}^{k_1}$ . Let  $\mathbf{w}_\ell^R = \text{Re}(\mathbf{w}_\ell)$  and  $\mathbf{w}_\ell^I = \text{Im}(\mathbf{w}_\ell)$ . These vectors are mapped to points  $\mathbf{t}_\ell^R, \mathbf{t}_\ell^I \in \Lambda_1 \cap \mathcal{V}$  as follows:

$$\mathbf{t}_\ell^R = [\mathbf{w}_\ell^R \mathbf{G}_1 \mathbf{L}] \bmod \Lambda \quad (12)$$

$$\mathbf{t}_\ell^I = [\mathbf{w}_\ell^I \mathbf{G}_1 \mathbf{L}] \bmod \Lambda \quad (13)$$

Each encoder is given two *dither vectors*,  $\mathbf{d}_\ell^R$  and  $\mathbf{d}_\ell^I$ , generated independently and uniformly from  $\mathcal{V}$  and also given to the receiver. Encoder  $\ell$  generates a channel input as follows:

$$\mathbf{x}_\ell = [\mathbf{t}_\ell^R - \mathbf{d}_\ell^R] \bmod \Lambda + j[\mathbf{t}_\ell^I - \mathbf{d}_\ell^I] \bmod \Lambda \quad (14)$$

The dither vectors ensure that  $\mathbf{x}_\ell$  is the sum of two independent vectors that are uniform over the coarse Voronoi region and thus  $E[||\mathbf{x}_\ell||^2] = \text{SNR}$ . The channel output is given by  $\mathbf{y} = \sum_{\ell=1}^L h_\ell \mathbf{x}_\ell + \mathbf{z}$ . Assume that the decoder would like to decode the message equation  $\bigoplus_{\ell=1}^L q_\ell \mathbf{w}_\ell$ . We define the following two quantities:

$$\mathbf{v}^R = \left[ \sum \text{Re}(q_\ell) \mathbf{t}_\ell^R - \text{Im}(q_\ell) \mathbf{t}_\ell^I \right] \bmod \Lambda \quad (15)$$

$$\mathbf{v}^I = \left[ \sum \text{Im}(q_\ell) \mathbf{t}_\ell^R + \text{Re}(q_\ell) \mathbf{t}_\ell^I \right] \bmod \Lambda. \quad (16)$$

These are equations of the lattice points (not the message symbols). We will see later that it is easy to go from these lattice equations to the desired message equations. The decoder scales the channel output by some  $\alpha \in \mathbb{C}$  and estimates the lattice equations as follows:

$$\hat{\mathbf{v}}^R = [Q_1(\text{Re}(\alpha \mathbf{y}) + \sum_{\ell=1}^L \text{Re}(q_\ell) \mathbf{d}_\ell^R - \text{Im}(q_\ell) \mathbf{d}_\ell^I)] \bmod \Lambda$$

$$\hat{\mathbf{v}}^I = [Q_1(\text{Im}(\alpha \mathbf{y}) + \sum_{\ell=1}^L \text{Im}(q_\ell) \mathbf{d}_\ell^R + \text{Re}(q_\ell) \mathbf{d}_\ell^I)] \bmod \Lambda$$

where  $Q_1(\cdot)$  is the nearest neighbor quantizer for  $\Lambda_1$ . Although there are multiple transmitters, due to the linear structure of the lattice, we can also view  $\mathbf{y}$  as a noisy version of the lattice codewords. Using Lemma 2 from [2], we can show that the

channels from  $\mathbf{v}^R$  to  $\hat{\mathbf{v}}^R$  and from  $\mathbf{v}^I$  to  $\hat{\mathbf{v}}^I$  are equivalent in distribution to:

$$\hat{\mathbf{v}}^R = [Q_1([\mathbf{v}^R + \mathbf{z}_{eq}^R] \bmod \Lambda)] \bmod \Lambda \quad (17)$$

$$\hat{\mathbf{v}}^I = [Q_1([\mathbf{v}^I + \mathbf{z}_{eq}^I] \bmod \Lambda)] \bmod \Lambda \quad (18)$$

$$\mathbf{z}_{eq}^R = \tilde{\mathbf{z}}^R + \sum_{\ell=1}^L \text{Re}(\alpha h_\ell - q_\ell) \tilde{\mathbf{d}}_\ell^R - \text{Im}(\alpha h_\ell - q_\ell) \tilde{\mathbf{d}}_\ell^I \quad (19)$$

$$\mathbf{z}_{eq}^I = \tilde{\mathbf{z}}^I + \sum_{\ell=1}^L \text{Im}(\alpha h_\ell - q_\ell) \tilde{\mathbf{d}}_\ell^R + \text{Re}(\alpha h_\ell - q_\ell) \tilde{\mathbf{d}}_\ell^I \quad (20)$$

where  $\tilde{\mathbf{z}}^R$  and  $\tilde{\mathbf{z}}^I$  are distributed according to  $\mathcal{N}(\mathbf{0}, |\alpha|^2 \mathbb{I}^{n \times n})$  and each  $\tilde{\mathbf{d}}_\ell^R$  and  $\tilde{\mathbf{d}}_\ell^I$  is drawn independently and uniformly from  $\mathcal{V}$ . It can also be shown that:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \|\mathbf{z}_{eq}^R\|^2 = \lim_{n \rightarrow \infty} \frac{1}{n} \|\mathbf{z}_{eq}^I\|^2 = \frac{1}{2} (|\alpha|^2 + \text{SNR} \|\alpha \mathbf{h} - \mathbf{q}\|^2)$$

We can now characterize the achievable rate for recovering a single equation of lattice points. It then remains to prove that this lattice equation is equivalent to the desired message equation.

*Theorem 1:* For any  $\epsilon > 0$  and  $n$  large enough, there exists a nested lattice pair  $\Lambda \subset \Lambda_1$  with  $R_1 - \epsilon < k_1 n^{-1} 2 \log_2 p < R_1$  where

$$R_1 = \log^+ \left( \frac{\text{SNR}}{|\alpha|^2 + \text{SNR} \|\alpha \mathbf{h} - \mathbf{q}\|^2} \right) \quad (21)$$

such that the lattice equation  $\mathbf{v}^R + j\mathbf{v}^I$  can be recovered from the channel output  $\mathbf{y}$  with probability of error upper bounded by  $\epsilon$ :

$$\Pr(\hat{\mathbf{v}}^R + j\hat{\mathbf{v}}^I \neq \mathbf{v}^R + j\mathbf{v}^I) < \epsilon. \quad (22)$$

The proof relies on showing that the equivalent noise terms  $\mathbf{z}_{eq}^R$  and  $\mathbf{z}_{eq}^I$  are no worse than Gaussian noise with the same variance. Furthermore, we use the fact that lattice decoding (for real-valued channels) is successful at any rate less than  $\frac{1}{2} \log \left( \frac{P}{N_{eq}} \right)$  where  $P$  is the transmit power and  $N_{eq}$  is the equivalent noise power. The real and imaginary lattice components use power  $\text{SNR}/2$  each and  $N_{eq} = \frac{1}{2} (|\alpha|^2 + \text{SNR} \|\alpha \mathbf{h} - \mathbf{q}\|^2)$ . Since we have both real and imaginary components, we arrive at  $R_1$  for the achievable rate. A full proof will appear in the journal version.

*Lemma 1:* For a given  $\mathbf{h} \in \mathbb{C}^L$ ,  $\mathbf{q} \in \{\mathbb{F}_p + j\mathbb{F}_p\}^L$ , and  $\text{SNR} > 0$ , the compute-and-forward rate given by

$$R_1 = \log^+ \left( \frac{\text{SNR}}{|\alpha|^2 + \text{SNR} \|\alpha \mathbf{h} - \mathbf{q}\|^2} \right) \quad (23)$$

is uniquely maximized by choosing  $\alpha$  to be the MMSE coefficient

$$\alpha_{\text{opt}} = \frac{\text{SNR} \mathbf{h}^* \mathbf{q}}{1 + \text{SNR} \|\mathbf{h}\|^2} \quad (24)$$

which results in a rate

$$R_{1,\text{opt}} = -\log^+ \left( \|\mathbf{q}\|^2 - \frac{\text{SNR} \|\mathbf{h}^* \mathbf{q}\|^2}{1 + \text{SNR} \|\mathbf{h}\|^2} \right) \quad (25)$$

Note that  $|\alpha|^2 + \text{SNR}\|\alpha\mathbf{h} - \mathbf{q}\|^2$  is quadratic in  $\alpha$ . The optimizing  $\alpha$  is simply found by setting the first derivative equal to zero. We then just plug back into the expression for  $R_1$ .

Note that our scheme only requires channel knowledge at the receiver. The transmitters only need to know their respective rate targets.

We will now show that we can recover the message equation  $\mathbf{u} = \bigoplus_{\ell=1}^L q_\ell \mathbf{w}_\ell$  from the decoded lattice equation  $\mathbf{v}^R + \mathbf{v}^I$ .

*Lemma 2:* Given the real and imaginary parts of the recovered lattice equation,  $\mathbf{v}^R$  and  $\mathbf{v}^I$ , we can recover the desired message equation  $\mathbf{u} = \bigoplus_{\ell=1}^L q_\ell \mathbf{w}_\ell$  using the following transformation:

$$\mathbf{c}^R = p([\mathbf{v}^R \mathbf{L}^{-1}] \bmod \mathbb{Z}^n) \quad (26)$$

$$\mathbf{c}^I = p([\mathbf{v}^I \mathbf{L}^{-1}] \bmod \mathbb{Z}^n) \quad (27)$$

$$\mathbf{u} = \mathbf{c}^R \mathbf{G}_1^T (\mathbf{G}_1 \mathbf{G}_1^T)^{-1} + j (\mathbf{c}^I \mathbf{G}_1^T (\mathbf{G}_1 \mathbf{G}_1^T)^{-1}) \quad (28)$$

where matrix operations in (28) are over  $\mathbb{F}_p$  and all other operations are over  $\mathbb{C}$ .

*Proof:* Recall that the transmitted lattice points  $\mathbf{t}_\ell^R$  and  $\mathbf{t}_\ell^I$  are generated from the message symbols according to (12) and (13). It is easy to show that  $\mathbf{L}$  is full rank since by default Construction A includes all unit vectors as elements of the lattice. Furthermore,  $\mathbf{L}^{-1}$  moves all points quantized by  $Q(\cdot)$  back onto points in  $\mathbb{Z}^n$ . We have that:

$$\begin{aligned} \mathbf{t}_\ell^R &= p^{-1} \mathbf{w}_\ell^R \mathbf{G}_1 \mathbf{L} - Q(p^{-1} \mathbf{w}_\ell^R \mathbf{G}_1 \mathbf{L}) \\ \mathbf{t}_\ell^R \mathbf{L}^{-1} &= p^{-1} \mathbf{w}_\ell^R \mathbf{G}_1 - Q(p^{-1} \mathbf{w}_\ell^R \mathbf{G}_1 \mathbf{L}) \mathbf{L}^{-1} \\ [\mathbf{t}_\ell^R \mathbf{L}^{-1}] \bmod \mathbb{Z}^n &= p^{-1} \mathbf{w}_\ell^R \mathbf{G}_1 \end{aligned}$$

Using this identity and a similar one for  $\mathbf{t}_\ell^I$  we can get that:

$$\mathbf{c}^R = p[\mathbf{v}^R \mathbf{L}^{-1}] \bmod \mathbb{Z}^n \quad (29)$$

$$= \bigoplus_{\ell=1}^L (\text{Re}(q_\ell) \mathbf{w}_\ell^R - \text{Im}(q_\ell) \mathbf{w}_\ell^I) \mathbf{G}_1 \quad (30)$$

Finally, since  $\mathbf{G}_1$  is rank  $k_1$  we can apply the right inverse  $\mathbf{G}_1^T (\mathbf{G}_1 \mathbf{G}_1^T)^{-1}$  to recover  $\mathbf{u}^R = \bigoplus_{\ell} (\text{Re}(q_\ell) \mathbf{w}_\ell^R - \text{Im}(q_\ell) \mathbf{w}_\ell^I)$ . Using similar steps, we can recover  $\mathbf{u}^I = \bigoplus_{\ell} (\text{Im}(q_\ell) \mathbf{w}_\ell^R + \text{Re}(q_\ell) \mathbf{w}_\ell^I)$ . These are just the real and imaginary parts of the desired message equation and we get that  $\mathbf{u} = \mathbf{u}^R + j\mathbf{u}^I$ . ■

## V. MULTIPLE RECEIVER COMPUTE-AND-FORWARD

We now generalize our results to the multiple receiver case. Again, we limit ourselves to a single message level.

*Theorem 2:* Assume each receiver is interested in the message equation  $\mathbf{u}_m = \bigoplus_{\ell=1}^L q_{m\ell} \mathbf{w}_\ell$ . For any  $\epsilon > 0$  and  $n$  large enough, there exists a nested lattice pair  $\Lambda \subset \Lambda_1$  with  $R_{\text{COMP}} - \epsilon < k_1 n^{-1} 2 \log_2 p < R_{\text{COMP}}$  where

$$R_{\text{COMP}} = \min_{m=1,2,\dots,M} R_m \quad (31)$$

$$R_m = -\log^+ \left( \|\mathbf{q}_m\|^2 - \frac{\text{SNR}\|\mathbf{h}_m^* \mathbf{q}_m\|^2}{1 + \text{SNR}\|\mathbf{h}_m\|^2} \right) \quad (32)$$

such that each receiver can recover its message equation with total probability of error upper bounded by  $\epsilon$ :

$$\Pr(\{\hat{\mathbf{u}}_1 \neq \mathbf{u}_1\} \cup \dots \cup \{\hat{\mathbf{u}}_M \neq \mathbf{u}_M\}) < \epsilon. \quad (33)$$

The proof follows by ensuring that the rate satisfies the conditions in Theorem 1 for each receiver and applying Lemma 2 to recover the message equations from the lattice equations. We also use Lemma 1 to find the optimal scaling coefficients  $\alpha_m$  for each channel output prior to decoding. Again, note that the transmitters only need knowledge of the target rate, not the channel coefficients themselves.

## VI. MULTIPLE MESSAGE LEVELS

We now examine the case with several message levels ( $B \geq 1$ ). We need a bit more notation to express our achievable rates. Receiver  $m$  is interested in decoding a subset of the message level  $\mathcal{I}_m^D$ . This subset is ordered such that the first element is the first message level to be decoded. Let  $\mathcal{I}_{m,\beta}^D$  denote the first  $\beta$  elements of  $\mathcal{I}_m^D$ . Let  $\mathcal{U}_m$  denote the message levels which have coefficient vectors equal to some unit vector at receiver  $m$ .

Our encoding strategy for each level is as follow. Encoder  $\ell$  generates  $\mathbf{x}_{\ell,b}$  for each  $b \in \mathcal{I}_\ell^E$  just as in (14):

$$\mathbf{x}_{\ell,b} = [\mathbf{t}_{\ell,b}^R - \mathbf{d}_{\ell,b}^R] \bmod \Lambda + j[\mathbf{t}_{\ell,b}^I - \mathbf{d}_{\ell,b}^I] \bmod \Lambda \quad (34)$$

Each level uses  $0 \leq \gamma_{\ell,b} \leq 1$  fraction of the total power SNR. These are chosen to sum to one so that the power constraint is not violated:

$$\sum_{b \in \mathcal{I}_\ell^E} \gamma_{\ell,b} = 1 \quad (35)$$

The transmitted vector is just a weighted sum of the  $\mathbf{x}_{\ell,b}$ :

$$\mathbf{x}_\ell = \sum_{b \in \mathcal{I}_\ell^E} \sqrt{\gamma_{\ell,b}} \mathbf{x}_{\ell,b}. \quad (36)$$

Finally, we let  $\mathbf{h}_{m,b} = [\sqrt{\gamma_{1,b}} h_{m1} \dots \sqrt{\gamma_{L,b}} h_{mL}]^T$ . This allows us to adjust the power allocation into the channel coefficients and treat the entire system as if it operates under one coarse lattice with second moment SNR. Consider the case where receiver  $m$  is interested in decoding element  $\beta$  from its decoding set having decoded the previous  $\beta - 1$  message equations already. We will treat the remaining levels in the set  $\mathcal{I}_m^D \setminus \mathcal{I}_{m,\beta}^D$  as noise. Those message equations whose coefficient vectors are simply unit vectors (i.e. the message levels in  $\mathcal{U}_m$ ) can be completely removed from the channel output. Finally, those equations we have already decoded in  $\mathcal{I}_{m,\beta-1}^D$  can be partially removed. Unfortunately, since the lattice structure forces us to decode to integer coefficients we cannot always match the coefficient vectors to the channel vectors. Even upon successful decoding of an equation, we do not know the equation according to the channel coefficients, only the integer coefficients. Thus, when we strip off an equation after successful decoding, we are still left with the difference between the channel coefficients and equation coefficients as noise.

*Theorem 3:* Choose a receiver  $m$  with decoding order  $\mathcal{I}_m^D$ . For any  $\epsilon > 0$ ,  $\alpha_{m,\beta} \in \mathbb{C}$ , and  $n$  large enough, there exists a coarse lattice  $\Lambda$  and a set of fine lattices  $\Lambda_1, \dots, \Lambda_B$  each satisfying  $R_{m,\beta} - \epsilon < k_\beta n^{-1} 2 \log_2 p < R_{m,\beta}$  where

$$N_{m,\beta} = \left( 1 + \text{SNR} \sum_{b \in \mathcal{I}_m^D \setminus \mathcal{I}_{m,\beta}^D} \|\mathbf{h}_{m,b}\|^2 \right) \quad (37)$$

$$A_{m,\beta} = \sum_{b \in \mathcal{I}_{m,\beta}^D \setminus \mathcal{U}_m} \|\alpha_{m,\beta} \mathbf{h}_{m,b} - \mathbf{q}_{m,b}\|^2 \quad (38)$$

$$R_{m,\beta} = \log^+ \left( \frac{\text{SNR}}{|\alpha_{m,\beta}|^2 N_{m,\beta} + \text{SNR} A_{m,\beta}} \right) \quad (39)$$

such that receiver  $m$  can make estimates  $\hat{\mathbf{u}}_{m,b}$  of message equations  $\mathbf{u}_{m,b} = \bigoplus_{\ell=1}^L q_{m\ell,b} \mathbf{w}_{\ell,b}$  with total probability of error upper bounded by  $\epsilon$ :

$$\Pr \left( \bigcup_{b \in \mathcal{I}_m^D} \{\hat{\mathbf{u}}_{m,b} \neq \mathbf{u}_{m,b}\} \right) < \epsilon. \quad (40)$$

A full proof will appear in the journal version. Also note that the maximizing  $\alpha_{m,\beta}$  can be derived by setting the first derivative to zero as it is again a quadratic program.

*Theorem 4:* Each receiver  $m$  is interested in decoding message equation  $\mathbf{u}_{m,b} = \bigoplus_{\ell=1}^L q_{m\ell,b} \mathbf{w}_{\ell,b}$  at message level  $b$  and has a decoding order  $\mathcal{I}_b^D$ . For any  $\epsilon > 0$  and  $n$  large enough, there exists a coarse lattice  $\Lambda$  and fine lattices  $\Lambda_1, \dots, \Lambda_B$  each satisfying  $R_\beta - \epsilon < k_\beta n^{-1} 2 \log_2 p < R_\beta$  where

$$R_\beta = \min_{\forall m \text{ s.t. } \beta \in \mathcal{I}_m^D} R_{m,\beta} \quad (41)$$

with  $R_{m,\beta}$  given by (39) such that every receiver can make estimates  $\hat{\mathbf{u}}_{m,b}$  with total probability of error upper bounded by  $\epsilon$ :

$$\Pr \left( \bigcup_{m=1}^M \bigcup_{b \in \mathcal{I}_m^D} \{\hat{\mathbf{u}}_{m,b} \neq \mathbf{u}_{m,b}\} \right) < \epsilon. \quad (42)$$

This follows from by ensuring that each receiver is able to satisfy the conditions of Theorem 3. Theorem 4 is sufficient to form a complete description of achievable rates for recovering equations in any Gaussian network. It can be shown that the usual strategies of superposition and successive cancellation are a special case of Theorem 4 by simply choosing sufficiently many levels and setting all of the desired equations to be unit vectors.

A destination node simply needs to collect enough message equations to solve for the desired messages over  $\mathbb{F}_p$  and decoding will be successful at the rate of the given message level.

To maximize the rate in a given Gaussian network, we will have to optimize not only the number of levels and the appropriate power allocations but the coefficients of the message equations to be decoded. Although it seems like this optimization is only possible by exhaustive search, the solution space is in fact finite for a fixed SNR.

## VII. CONCLUSIONS

In this paper, we have developed a nested lattice compute-and-forward strategy so that nodes inside the network can recover equations of the original message symbols with vanishing probability of error. This can serve as an ideal framework for physical-layer network coding as well as distributed MIMO and other cooperative communication strategies. We have characterized the rates for sending these equations and extended our strategy to include both superposition and successive cancellation. Since the transmitters do not need to know the channel coefficients, this framework can easily be extended to the slow fading case by developing a notion of outage capacity for sending equations. This will be included in an upcoming journal submission.

## ACKNOWLEDGMENT

This work was supported in part by NSF grants CCR 0347298, CNS 0627024, and CCF 0830428.

## REFERENCES

- [1] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference with structured codes," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008)*, (Toronto, Canada), July 2008.
- [2] 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, pp. 2293–2314, October 2004.
- [3] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, pp. 1250–1276, June 2002.
- [4] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *European Transactions on Telecommunications*, 2008. To appear.
- [5] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Transactions on Information Theory*, vol. 25, pp. 219–221, March 1979.
- [6] B. Nazer and M. Gastpar, "Lattice coding increases multicast rates for Gaussian multiple-access networks," in *45th Annual Allerton Conference*, (Monticello, IL), September 2007.
- [7] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Transactions on Information Theory*, vol. 53, pp. 3498–3516, October 2007.
- [8] T. Philosof, A. Khisti, U. Erez, and R. Zamir, "Lattice strategies for the dirty multiple access channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2007)*, (Nice, France), June 2007.
- [9] G. Bresler, A. Parekh, and D. Tse, "The approximate capacity of a one-sided interference channel," in *45th Annual Allerton Conference*, (Monticello, IL), September 2007.
- [10] A. Sanderovich, M. Peleg, and S. Shamai, "Scaling laws in decentralized processing of interfered Gaussian channels," in *International Zurich Seminar on Communications (IZS 2008)*, (Zurich, Switzerland), March 2008.
- [11] K. Narayanan, M. P. Wilson, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," in *45th Annual Allerton Conference*, (Monticello, IL), September 2007.
- [12] D. Krithivasan and S. Pradhan, "Lattices for distributed source coding: Jointly Gaussian sources and reconstruction of a linear function," *IEEE Transactions on Information Theory*, Submitted July 2007. See <http://arxiv.org/abs/0707.3461>.
- [13] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Transactions on Information Theory*, vol. 51, pp. 3401–3416, October 2005.