Compute-and-Forward: Harnessing Interference through Structured Codes

Bobak Nazer, *Member, IEEE* and Michael Gastpar, *Member, IEEE*

***Abstract*—Interference is usually viewed as an obstacle to communication in wireless networks. This paper proposes a new strategy, compute-and-forward, that exploits interference to obtain significantly higher rates between users in a network. The key idea is that relays should decode linear functions of transmitted messages according to their observed channel coefficients rather than ignoring the interference as noise. After decoding these linear equations, the relays simply send them towards the destinations, which given enough equations, can recover their desired messages. The underlying codes are based on nested lattices whose algebraic structure ensures that integer combinations of codewords can be decoded reliably. Encoders map messages from a finite field to a lattice and decoders recover equations of lattice points which are then mapped back to equations over the finite field. This scheme is applicable even if the transmitters lack channel state information.**

***Index Terms*—Relaying, cooperative communication, structured codes, nested lattice codes, reliable computation, AWGN networks, interference.**

I. Introduction

In a wireless network, a transmission from a single node is heard not only by the intended receiver, but also by all other nearby nodes; by analogy, any receiver not only captures the signal from its designated transmitter, but from all other nearby transmitters. The resulting interference is usually viewed as highly undesirable and clever algorithms and protocols have been devised to avoid interference between transmitters. Collectively, these strategies transform the physical layer into a set of *reliable bit pipes*, i.e. each link can accommodate a certain number of bits per time unit. These bit pipes can then be used seamlessly by higher layers in the protocol stack.

Since wireless terminals must compete for the same fixed chunk of spectrum, interference avoidance results in diminishing rates as the network size increases. Recent work on cooperative communication has shown that this penalty can be overcome by adopting new strategies at the physical layer. The key idea is that users should help relay each other's messages by exploiting the broadcast and multiple-access properties of the wireless medium; properties that are usually viewed as a hindrance and are not captured by a bit pipe interface. To date, most proposed cooperative schemes have relied on one of the following three core relaying strategies:

- *Decode-and-Forward:* The relay decodes at least some part of the transmitted messages. The recovered bits are then re-encoded for collaborative transmission to the next relay. Although this strategy offers significant advantages, the relay is ultimately interference-limited as the number of transmitted messages increases [1]–[4].
- *Compress-and-Forward:* The signal observed at the relay is vector quantized and this information is passed towards the destination. If the destination receives information from multiple relays, it can treat the network as a multiple-input multiple-output (MIMO) channel. Unfortunately, since no decoding is performed at intermediate nodes, noise builds up as messages traverse the network [1], [3], [5]–[8].
- *Amplify-and-Forward:* The relay simply acts as a repeater and transmits a scaled version of its observation. Like compress-and-forward, this strategy converts the network into a large MIMO channel with the added possibility of a beamforming gain. However, noise also builds up with each retransmission. [2], [4], [9]–[12].

In this paper, we propose a new strategy, *compute-and-forward*, that enables relays to decode linear equations of the transmitted messages using the noisy linear combinations provided by the channel. A destination, given sufficiently many linear combinations, can solve for its desired messages. Our strategy relies on codes with a linear structure, specifically nested lattice codes. The linearity of the codebook ensures that integer combinations of codewords are themselves codewords. A relay is free to determine which linear equation to recover, but those closer to the channel's fading coefficients are available at higher rates.

This strategy simultaneously affords protection against noise and the opportunity to exploit interference for cooperative gains. One could interpret compress-and-forward and amplify-and-forward as converting a network into a set of noisy linear equations; in this sense, compute-and-forward converts it into a set of *reliable linear equations*. These equations can in turn be used for a digital implementation of cooperative schemes that could fit into a (slightly revised) network protocol stack. Classical relaying strategies seem to require a cross-layer design that dispenses with bit pipes and gives higher layers in the network stack direct access to the wireless medium.

This work was supported by the National Science Foundation under grants CCR 0347298, CNS 0627024, and CCF 0830428 as well a Graduate Research Fellowship. M. Gastpar was also supported by the European Research Council under grant ERC StG 259530-ComCom. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Toronto, Canada, July 2008 and at the 42nd Annual IEEE Asilomar Conference on Signals, Systems, and Computers, Monterey, CA, October 2008.

B. Nazer is with the Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA (email: bobak@bu.edu). M. Gastpar is with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720 USA, and with the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale (EPFL), 1015 Lausanne, Switzerland (e-mail: gastpar@eecs.berkeley.edu).

However, this would negate many of the advantages of a modular design [13]. Compute-and-forward provides a natural solution to this problem by permitting a slight revision of the interface from bits to *equations of bits*.

We will develop a general framework for compute-and-forward that can be used in any relay network with linear channels and additive white Gaussian noise (AWGN). Transmitters send out messages taking values in a prime-sized finite field and relays recover linear equations of the messages over the same field, making this an ideal physical layer interface for network coding. We will compare compute-and-forward to classical relaying strategies in a case study based on distributed MIMO. Classical relaying strategies perform well in either low or high signal-to-noise ratio (SNR) regimes. As we will see, compute-and-forward offers advantages in moderate SNR regimes where both interference and noise are significant factors.

A. Related Work

There is a large body of work on lattice codes and their applications in communications. We cannot do justice to all of this work here and point the interested reader to an excellent survey by Zamir [14]. The basic insight is that, for many AWGN networks of interest, nested lattice codes can approach the performance of standard random coding arguments. One key result by Erez and Zamir showed that nested lattice codes (combined with lattice decoding) can achieve the capacity of the point-to-point AWGN channel [15]. More generally, Zamir, Shamai, and Erez demonstrated how to use nested lattice codes for many classical AWGN multi-terminal problems in [16]. Subsequent work by El Gamal, Caire, and Damen showed that nested lattice codes achieve the diversity-multiplexing tradeoff of MIMO channels [17]. Note that, in general, structured codes are not sufficient to prove capacity results. For instance, group codes cannot approach the capacity of asymmetric discrete memoryless channels [18].

It is tempting to assume that requiring codes to have a certain algebraic structure diminishes their usefulness for proving capacity theorems. However, it has become clear that for certain network communication scenarios, structured codes can actually outperform standard random coding arguments [19]. The first example of such behavior was found by Körner and Marton in [20]. They considered a decoder that wants to reconstruct the parity of two dependent binary sources observed by separate encoders. They found the rate region by using the same linear code at each encoder. More recently, we showed that structured codes offer large gains for reliable computation over multiple-access channels [21]. Philosof *et al.* demonstrated that structured codes enable distributed dirty paper coding for multiple-access channels [22], [23].

The celebrated paper of Ahlswede *et al.* on network coding showed that for wired networks, relays must send out functions of received data, rather than just routing it [24]. Subsequent work has shown that linear codes [25], [26] and linear codes with random coefficients [27] are sufficient for multicasting. There has recently been a great deal of interest in exploiting the physical layer of the wireless medium for network coding. To the best of our knowledge, the idea of using wireless interference for network coding was independently and concurrently proposed by several groups. Zhang, Liew, and Lam developed modulation strategies for bi-directional communication and coined the phrase ”physical layer network coding” [28]. Popovski and Yomo suggested the use of amplify-and-forward for the two-way relay channel [29]. For this network, Rankov and Wittneben suggested both amplify-and-forward and compress-and-forward [30]. We suggested the use of structured codes for the closely related wireless butterfly network [31]. Subsequently, we developed lattice strategies for Gaussian multiple-access networks (without fading) [32] and Narayanan, Wilson, and Sprintson developed a nested lattice strategy for the two-way relay channel [33], [34]. Nam, Chung, and Lee generalized this strategy to include asymmetric power constraints [35], found the capacity to within half a bit [36], and extended their scheme to Gaussian multiple-access networks [37]. Owing to space constraints, we point to surveys by Liew, Zhang, and Lu [38] and ourselves [39] for a broader view of the rest of the physical layer network coding literature.

Work on interference alignment by Maddah-Ali, Motahari, and Khandani [40] and Cadambe and Jafar [41] has shown that large gains are possible for interference channels at high signal-to-noise ratio (SNR). The key is to have users transmit along subspaces chosen such that all interference stacks up in the same dimensions at the receivers. Lattice codes can be used to realize these gains at finite SNR. Bresler, Parekh, and Tse used lattice codes to approximate the capacity of the many-to-one and one-to-many interference channels to within a constant number of bits [42]. This scheme was employed for bursty interference channels in [43]. For symmetric interference channels, Sridharan *et al.* developed a layered lattice strategy in [44]. Structured codes are also useful for ergodic alignment over fast fading interference channels [45] and multi-hop networks [46] as well as decentralized processing in cellular networks [47], [48].

Distributed source coding can also benefit from the use of structured codes. Krithivasan and Pradhan have employed nested lattice codes for the distributed compression of linear functions of jointly Gaussian sources [49] as well as nested group codes for discrete memoryless sources [50]. Wagner improved the performance of this lattice scheme in the low rate regime via binning and developed novel outer bounds [51].

Large gains are possible in multi-user source-channel coding [52]–[54]. For Gaussian settings, the modulo-lattice modulation scheme of Kochman and Zamir is particularly useful [55]. Finally, recent work by He and Yener has shown that lattices are useful for physical layer secrecy [56]. See also [57].

Finally, we mention several recent papers that have developed practical codes for compute-and-forward [58]–[60].

B. Summary of Paper Results

Our basic strategy is to take messages from a finite field, map them onto lattice points, and transmit these across the channel. Each relay observes a linear combination of these lattice points and attempts to decode an integer combination of them. This equation of lattice points is finally mapped back

to a linear equation over a finite field. Our main theorems are summarized below:

- Theorems 1 and 2 give our achievable rates for sending equations over a finite field from transmitters to relays over real-valued channel models. The strategy relies on a nested lattice coding strategy which is developed in Theorem 5. The corresponding results for complex-valued channel models are stated in Theorems 3, 4, and 6.
- Theorems 7 through 11 give sufficient conditions on the equation coefficients so that a destination can recover one or more of the original messages.
- Theorems 12 and 13 generalize the compute-and-forward scheme to include successive cancellation and superposition coding.
- Theorem 14 is a simple upper bound on the rates for sending equations.

We extend our framework to the slow fading setting in Section IX. We then compare the performance of compute-and-forward to that of classical relaying strategies via a distributed MIMO case study in Section X.

II. Problem Statement

Our relaying strategy is applicable to any configuration of sources, relays, and destinations that are linked through linear[1] channels with additive white Gaussian[2] noise (AWGN). We will refer to such configurations as AWGN networks. To simplify the description of the scheme, we will first focus on how to deliver equations to a single set of relays. 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 AWGN network. We will begin with definitions for real-valued channel models and then modify these to fit complex-valued channel models.

A. Real-Valued Channels

Let $\mathbb{R}$ denote the reals and $\mathbb{F}_p$ denote the finite field of size p where p is always assumed to be prime. Let $+$ denote addition over the reals and $\oplus$ addition over the finite field. Furthermore, let $\sum$ denote summation over the reals and $\bigoplus$ denote summation over the finite field. It will be useful to map between the prime-sized finite field $\mathbb{F}_p$ and the corresponding subset of the integers, $\{0, 1, 2, \ldots, p-1\}$. We will use the function $g(\cdot)$ to denote this map. This is essentially an identity map except for the change of alphabet. If g or its inverse g^{-1} are applied to a vector we assume they operate element-wise. We assume that the $\log$ operation is with respect to base 2.

We will use boldface lowercase letters to denote column vectors and boldface uppercase letters to denote matrices. For example, $\mathbf{h} \in \mathbb{R}^L$ and $\mathbf{H} \in \mathbb{R}^{M \times L}$. Let $\|\mathbf{h}\| \triangleq \sqrt{\sum_{i=1}^{L} |h[i]|^2}$ denote the ℓ^2-norm of $\mathbf{h}$. Also, let $\mathbf{h}^T$ denote the transpose of $\mathbf{h}$. Finally, let $\mathbf{0}$ denote the zero vector, δ_ℓ denote the unit vector with 1 in the ℓ^{th} entry and 0 elsewhere, and $\mathbf{I}^{M \times M}$ denote the identity matrix of size M.

Definition 1 (Messages): Each transmitter (indexed by $\ell = 1, 2, \ldots, L$) has a length-k_ℓ *message vector* that is drawn independently and uniformly over a prime-size finite field, $\mathbf{w}_\ell \in \mathbb{F}_p^{k_\ell}$. Without loss of generality, we assume that the transmitters are indexed by increasing message length. Since we are interested in functions of these message vectors, we zero-pad them to a common length $k \triangleq \max_\ell k_\ell$.

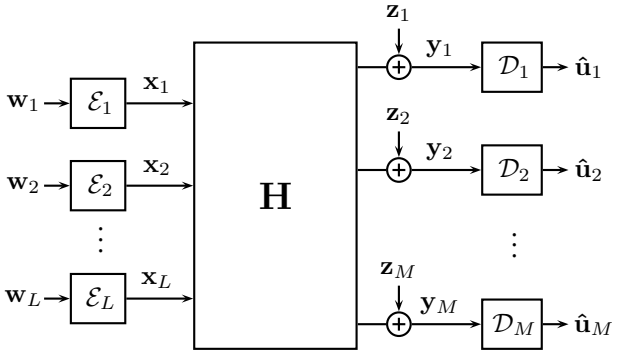

Fig. 1. L transmitters reliably communicate linear functions $\mathbf{u}_m = \bigoplus_{\ell=1}^{L} q_{m\ell}\mathbf{w}_\ell$ to M relays over a real-valued AWGN network.

Definition 2 (Encoders): Each transmitter is equipped with an *encoder*, $\mathcal{E}_\ell : \mathbb{F}_p^k \to \mathbb{R}^n$, that maps length-$k$ messages over the finite field to length-n real-valued codewords, $\mathbf{x}_\ell = \mathcal{E}(\mathbf{w}_\ell)$. Each codeword is subject to the usual *power constraint*,

$$\|\mathbf{x}_\ell\|^2 \le nP \ . \tag{1}$$

Remark 1: Note that asymmetric power constraints can be incorporated by scaling the channel coefficients appropriately.

Definition 3 (Message Rate): The *message rate* R_ℓ of each transmitter is the length of its message (measured in bits) normalized by the number of channel uses,

$$R_\ell = \frac{k_\ell}{n} \log p \ . \tag{2}$$

Note that with our choice of indexing, the rates are in decreasing order, $R_1 \ge R_2 \ge \cdots \ge R_L$.

Definition 4 (Channel Model): Each relay (indexed by $m = 1, 2, \ldots, M$) observes a noisy linear combination of the transmitted signals through the *channel*,

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

where $h_{m\ell} \in \mathbb{R}$ are the channel coefficients and $\mathbf{z}$ is i.i.d. Gaussian noise, $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}^{n \times n})$. Let $\mathbf{h}_m = [h_{m1} \cdots h_{mL}]^T$ denote the vector of channel coefficients to relay m and let $\mathbf{H} = \{h_{m\ell}\}$ denote the entire channel matrix. Note that by this convention the m^{th} row of $\mathbf{H}$ is $\mathbf{h}_m^T$.

Remark 2: For our initial analysis, we will assume that the channel coefficients are fixed for all time. However, these results can easily be extended to the slow fading case under an outage formulation which we develop in Section IX.

[1] Erez and Zamir have recently investigated applying this framework to non-linear scenarios [61].

[2] In fact, our strategy is applicable to a much broader class of additive noise statistics since we employ a minimum-distance decoder.

Remark 3: Our coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know $\mathbf{h}_m$. Each transmitter only needs to know the desired message rate, not the realization of the channel.

Definition 5 (Desired Equations): The goal of each relay is to reliably recover a *linear combination* of the messages

$$\mathbf{u}_m = \bigoplus_{\ell=1}^{L} q_{m\ell}\mathbf{w}_\ell \ . \tag{4}$$

where $q_{m\ell}$ are coefficients taking values in $\mathbb{F}_p$. Each relay is equipped with a *decoder*, $\mathcal{D}_m : \mathbb{R}^n \to \mathbb{F}_p^k$, that maps the observed channel output $\mathbf{y}_m$ to an estimate $\hat{\mathbf{u}}_m = \mathcal{D}_m(\mathbf{y}_m)$ of the equation $\mathbf{u}_m$.

Although our desired equations are evaluated over the finite field $\mathbb{F}_p$, the channel operates over the reals $\mathbb{R}$. Our coding scheme will allow us to efficiently exploit the channel for reliable computation if the desired equation coefficients are close to the channel coefficients in an appropriate sense. The definition below provides an embedding from the finite field to the reals that will be useful in quantifying this closeness.

Definition 6 (Coefficient Vector): The *equation with coefficient vector* $\mathbf{a}_m = [a_{m1}\ a_{m2}\ \cdots\ a_{mL}]^T \in \mathbb{Z}^L$ is the linear combination of the transmitted messages $\mathbf{u}_m$ with coefficients given by

$$q_{m\ell} = g^{-1}\big([a_{m\ell}] \mod p\big) \ . \tag{5}$$

Recall that g^{-1} maps elements of $\{0, 1, 2, \ldots, p-1\}$ to the corresponding element in $\mathbb{F}_p$.

Definition 7 (Probability of Error): We say that the equations with coefficient vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_M \in \mathbb{Z}^L$ are decoded with *average probability of error* ϵ if

$$\Pr\left(\bigcup_{m=1}^{M} \{\hat{\mathbf{u}}_m \neq \mathbf{u}_m\}\right) < \epsilon \ . \tag{6}$$

We would like to design a coding scheme that allows the transmitters to be oblivious of the channel coefficients and enables the relays to use their channel state information to select which equation to decode. Intuitively, equations whose coefficient vectors closely approximate the channel coefficients will be available at the highest rates.

Definition 8 (Computation Rate): We say that the *computation rate region* $\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m)$ is achievable if for any $\epsilon > 0$ and n large enough, there exist encoders and decoders, $\mathcal{E}_1, \ldots, \mathcal{E}_L, \mathcal{D}_1, \ldots, \mathcal{D}_M$, such that all relays can recover their desired equations with average probability of error ϵ so long as the underlying message rates $R_1, \ldots, R_L$ satisfy

$$R_\ell < \min_{m:a_{m\ell}\neq 0} \mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) \ . \tag{7}$$

In other words, a relay can decode an equation if the involved messages (i.e. those with non-zero coefficients) have message rates less than the computation rate between the channel and equation coefficient vectors. In fact, a relay will often be able to decode more than one equation and will have to decide which to forward into the network based on the requirements of the destinations.

Although our scheme can be employed in any AWGN network, we will omit formal definitions for such networks and simply give recoverability conditions for equations of messages collected by a destination. This may occur via a single layer of relays as described above or through multiple layers.

Definition 9 (Recovery): We say that message $\mathbf{w}_\ell \in \mathbb{F}_p^{k_\ell}$ can be *recovered* at rate R_ℓ from the equations $\mathbf{u}_m$ with coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_M \in \mathbb{Z}^L$ if for any $\epsilon > 0$ and n large enough, there exists a decoder $\mathcal{D} : \{\mathbb{F}_p^k\}^M \to \mathbb{F}_p^{k_\ell}$ such that

$$\hat{\mathbf{w}}_\ell = \mathcal{D}\left(\mathbf{u}_1, \ldots, \mathbf{u}_M\right) \tag{8}$$

$$\Pr\left(\hat{\mathbf{w}}_\ell \neq \mathbf{w}_\ell\right) < \epsilon \ . \tag{9}$$

B. Complex-Valued Channels

Let $\mathbb{C}$ denote the complex field and $\mathbf{h}^*$ the Hermitian (or conjugate) transpose of a complex vector $\mathbf{h} \in \mathbb{C}^L$. We also define $j = \sqrt{-1}$. We are primarily interested in narrowband wireless channel models so we will specify our encoding and decoding schemes for complex baseband. Specifically, each transmitter sends a length-n complex vector $\mathbf{x}_\ell \in \mathbb{C}^n$, which must obey the power constraint $\|\mathbf{x}\|_2 \leq nP$. Each relay observes a noisy linear superposition of the codewords, $\mathbf{y}_m = \sum_\ell h_{m\ell}\mathbf{x}_\ell + \mathbf{z}_m$, where $h_{m\ell} \in \mathbb{C}$ are complex-valued channel coefficients and $\mathbf{z}_m$ is i.i.d. circularly symmetric complex Gaussian noise, $\mathbf{z}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}^{M\times M})$.

One simple possibility is to directly employ the framework developed above using the real-valued representation for complex vectors,

$$\mathsf{Re}(\mathbf{y}_m) = \sum_{\ell=1}^{L} \left(\mathsf{Re}(h_{m\ell})\mathsf{Re}(\mathbf{x}_\ell) - \mathsf{Im}(h_{m\ell})\mathsf{Im}(\mathbf{x}_\ell)\right) + \mathsf{Re}(\mathbf{z}_m)$$

$$\mathsf{Im}(\mathbf{y}_m) = \sum_{\ell=1}^{L} \left(\mathsf{Im}(h_{m\ell})\mathsf{Re}(\mathbf{x}_\ell) + \mathsf{Re}(h_{m\ell})\mathsf{Im}(\mathbf{x}_\ell)\right) + \mathsf{Im}(\mathbf{z}_m)$$

From here, we can treat a complex-valued network with L transmitters and M relays as a real-valued network with $2L$ transmitters and $2M$ relays. However, there is a more elegant solution that takes advantage of the special structure of complex symbols. Below, we modify definitions to fit the complex case.

Definition 10 (Complex Messages): Each transmitter has two length-k_ℓ vectors that are drawn independently and uniformly over a prime-size finite field, $\mathbf{w}_\ell^R, \mathbf{w}_\ell^I \in \mathbb{F}_p^{k_\ell}$. The superscript denotes whether the vector is intended for the real part or the imaginary part of the channel. Together these vectors are the *message* of transmitter ℓ, $\mathbf{w}_\ell = (\mathbf{w}_\ell^R, \mathbf{w}_\ell^I)$. As before, we assume that the transmitters are indexed by increasing message length and zero-pad them to a common length $k \triangleq \max_\ell k_\ell$ prior to encoding. The *message rate* of each transmitter is double the prior definition $R_\ell = (2k_\ell/n)\log p$.

Definition 11 (Desired Complex Equations): The goal of each relay is to reliably recover a *linear combination* of the

messages,

$$\mathbf{u}_m^R = \bigoplus_{\ell=1}^{L} \left(q_{m\ell}^R \mathbf{w}_\ell^R \oplus (-q_{m\ell}^I)\mathbf{w}_\ell^I \right) \tag{10}$$

$$\mathbf{u}_m^I = \bigoplus_{\ell=1}^{L} \left(q_{m\ell}^I \mathbf{w}_\ell^R \oplus q_{m\ell}^R \mathbf{w}_\ell^I \right) , \tag{11}$$

where the $q_{m\ell}$ are coefficients taking values in $\mathbb{F}_p$ and $(-q_{m\ell})$ denotes the additive inverse of $q_{m\ell}$. The *equation with coefficient vector* $\mathbf{a}_m = [a_{m1}\ a_{m2}\ \cdots\ a_{mL}]^T \in \{\mathbb{Z}+j\mathbb{Z}\}^L$ are the linear combinations with coefficients given by

$$q_{m\ell}^R = g^{-1}\big([\mathsf{Re}(a_{m\ell})] \bmod p \big) \tag{12}$$

$$q_{m\ell}^I = g^{-1}\big([\mathsf{Im}(a_{m\ell})] \bmod p \big). \tag{13}$$

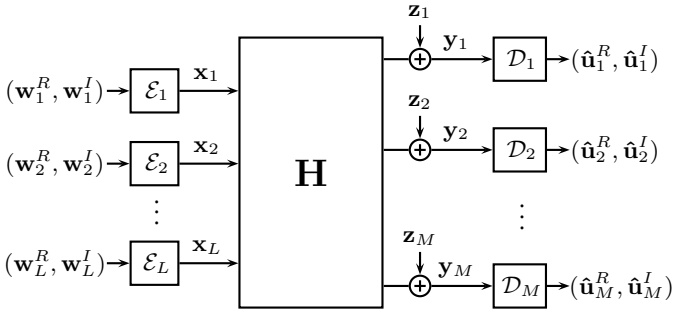

Fig. 2. L transmitters reliably communicate linear functions $\mathbf{u}_m^R = \bigoplus_{\ell=1}^{L} \left(q_{m\ell}^R \mathbf{w}_\ell^R \oplus (-q_{m\ell}^I)\mathbf{w}_\ell^I \right)$ and $\mathbf{u}_m^I = \bigoplus_{\ell=1}^{L} \left(q_{m\ell}^I \mathbf{w}_\ell^R \oplus q_{m\ell}^R \mathbf{w}_\ell^I \right)$ to M relays over a complex-valued AWGN network.

Note that the coefficient choices for the real and imaginary part are coupled, which means that each relay only needs to decide on $2L$ coefficients instead of the $4L$ needed for a real-valued system with $2L$ transmitters. The definitions for the probability of error, the computation rate region, and recovery are identical to Definitions 7, 8, and 9 except with $\mathbb{C}$ and $\{\mathbb{Z}+j\mathbb{Z}\}$ taking the place of $\mathbb{R}$ and $\mathbb{Z}$, respectively.

III. Main Results

Our main result is that relays can often recover an equation of messages at a higher rate than any individual message (or subset of messages). The rates are highest when the equation coefficients closely approximate the channel coefficients. Below, we give a formal statement of this result for real-valued channels. Let $\log^+(x) \triangleq \max(\log(x), 0)$.

Theorem 1: For real-valued AWGN networks with channel coefficient vectors $\mathbf{h}_m \in \mathbb{R}^L$ and equation coefficient vectors $\mathbf{a}_m \in \mathbb{Z}^L$, the following computation rate region is achievable:

$$\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) = \max_{\alpha_m \in \mathbb{R}} \frac{1}{2} \log^+ \left(\frac{P}{\alpha_m^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2} \right) .$$

A detailed proof is given in Section V-A.

Theorem 2: The computation rate given in Theorem 1 is uniquely maximized by choosing α_m to be the MMSE coefficient

$$\alpha_{\text{MMSE}} = \frac{P\ \mathbf{h}_m^T \mathbf{a}_m}{1 + P\|\mathbf{h}_m\|^2} \tag{14}$$

which results in a computation rate region of

$$\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) = \frac{1}{2} \log^+ \left(\left(\|\mathbf{a}_m\|^2 - \frac{P\ (\mathbf{h}_m^T \mathbf{a}_m)^2}{1 + P\|\mathbf{h}_m\|^2} \right)^{-1} \right)$$

The proof is nearly identical to that of Theorem 4.

The computation rate expression for the complex-valued case is simply twice the expression for the real-valued case.

Theorem 3: For complex-valued AWGN networks with channel coefficient vectors $\mathbf{h}_m \in \mathbb{R}^L$ and equation coefficient vectors $\mathbf{a}_m \in \{\mathbb{Z}+j\mathbb{Z}\}^L$, the following computation rate region is achievable:

$$\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) = \max_{\alpha_m \in \mathbb{C}} \log^+ \left(\frac{P}{|\alpha_m|^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2} \right) .$$

A detailed proof is given in Section V-B.

Theorem 4: The computation rate given in Theorem 3 is uniquely maximized by choosing α_m to be the MMSE coefficient

$$\alpha_{\text{MMSE}} = \frac{P\ \mathbf{h}_m^* \mathbf{a}_m}{1 + P\|\mathbf{h}_m\|^2} \tag{15}$$

which results in a computation rate region of

$$\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) = \log^+ \left(\left(\|\mathbf{a}_m\|^2 - \frac{P\ |\mathbf{h}_m^* \mathbf{a}_m|^2}{1 + P\|\mathbf{h}_m\|^2} \right)^{-1} \right) \tag{16}$$

Proof: Let $f(\alpha_m)$ denote the denominator of the computation rate in Theorem 3. Since it is quadratic in α_m, it can be uniquely minimized by setting its first derivative to zero.

$$f(\alpha_m) = \alpha_m^* \alpha_m + P(\alpha_m \mathbf{h}_m - \mathbf{a}_m)^*(\alpha_m \mathbf{h}_m - \mathbf{a}_m)$$

$$\frac{df}{d\alpha_m} = 2\alpha_m + P(2\alpha_m \mathbf{h}_m^* \mathbf{h}_m - 2\mathbf{h}_m^* \mathbf{a}_m) = 0 \tag{17}$$

$$\alpha_m (2 + 2P\|\mathbf{h}_m\|^2) = 2P\ \mathbf{h}_m^* \mathbf{a}_m \tag{18}$$

We solve this to get α_{MMSE} and plug back into $f(\alpha_m)$.

$$f(\alpha_{\text{MMSE}}) = \frac{P^2 |\mathbf{h}_m^* \mathbf{a}_m|^2}{(1 + P\|\mathbf{h}_m\|^2)^2} + \frac{P^3 \|\mathbf{h}_m\|^2 |\mathbf{h}_m^* \mathbf{a}_m|^2}{(1 + P\|\mathbf{h}_m\|^2)^2} - 2\frac{P^2 |\mathbf{h}_m^* \mathbf{a}_m|^2}{1 + P\|\mathbf{h}_m\|^2} + P\|\mathbf{a}_m\|^2 \tag{19}$$

$$= -\frac{P^2 |\mathbf{h}_m^* \mathbf{a}_m|^2}{1 + P\|\mathbf{h}_m\|^2} + P\|\mathbf{a}_m\|^2 \tag{20}$$

Substituting this into $\log^+\left(\frac{P}{f(\alpha_{\text{MMSE}})}\right)$ yields the desired computation rate. ∎

The main interpretation of Theorems 1 and 3 is that all relays can simultaneously decode equations with coefficient vectors $\mathbf{a}_m$ so long as the involved messages' rates are within the computation rate region

$$R_\ell < \min_{a_{m\ell} \neq 0} \mathcal{R}(\mathbf{h}_m, \mathbf{a}_m) . \tag{21}$$

In other words, exactly which equation to decode is left up to the relays. The scalar parameter α_m is used to move the channel coefficients closer to the desired integer coefficients. For instance, if $\alpha_m = 1$, then the effective signal-to-noise ratio is

$$\mathsf{SNR} = \frac{P}{1 + P\|\mathbf{h}_m - \mathbf{a}_m\|^2} ,$$

meaning that the non-integer part of the channel coefficients acts as additional noise. More generally, the scaled channel output $\alpha_m \mathbf{y}_m = \sum \alpha_m h_{m\ell} \mathbf{x}_\ell + \alpha_m \mathbf{z}_m$ can be equivalently written as a channel output $\tilde{\mathbf{y}}_m = \sum \tilde{h}_{m\ell} \mathbf{x}_\ell + \tilde{\mathbf{z}}_m$ where $\tilde{h}_{m\ell} = \alpha_m h_{m\ell}$ and $\tilde{\mathbf{z}}_m$ is i.i.d. according to $\mathcal{CN}(0, |\alpha_m|^2)$. In this case, the effective signal-to-noise ratio is

$$\mathsf{SNR} = \frac{P}{|\alpha_m|^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2} \ .$$

Since there is a rate penalty both for noise and for non-integer channel coefficients, then α_m should be used to optimally balance between the two as in Theorems 2 and 4. This is quite similar to the role of the MMSE scaling coefficient used by Erez and Zamir to achieve the capacity of the point-to-point AWGN channel in [15].

Example 1: Let the channel matrix take values on the complex integers, $\mathbf{H} \in \{\mathbb{Z} + j\mathbb{Z}\}^{M \times L}$, and assume that each relay wants a linear equation with a coefficient vector that corresponds exactly to the channel coefficients, $\mathbf{a}_m = \mathbf{h}_m$. Using Theorem 4, the relays can decode so long as

$$\begin{aligned} R_\ell &< \min_{m:h_{m\ell}\neq 0} \log^+ \left(\left(\|\mathbf{h}_m\|^2 - \frac{P\|\mathbf{h}_m\|^4}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right) \\ &= \min_{m:h_{m\ell}\neq 0} \log^+ \left(\frac{1+P\|\mathbf{h}_m\|^2}{\|\mathbf{h}_m\|^2 + P\|\mathbf{h}_m\|^4 - P\|\mathbf{h}_m\|^4} \right) \\ &= \min_{m:h_{m\ell}\neq 0} \log^+ \left(\frac{1}{\|\mathbf{h}_m\|^2} + P \right) \end{aligned} \tag{22}$$

Remark 4: One interesting special case of Example 1 is computing the modulo sum of codewords $\mathbf{w}_1 \oplus \mathbf{w}_2$ over a two-user Gaussian multiple-access channel $\mathbf{y} = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z}$. To date, the best known achievable computation rate for this scenario is $\log^+ \left(\frac{1}{2} + P\right)$. Several papers (including our own) have studied this special case and it is an open problem as to whether the best known outer bound $\log(1+P)$ is achievable [32], [34], [35]. Clearly, one can do better in the low SNR regime using standard multiple-access codes to recover all the messages then compute the sum to get $\frac{1}{2}\log(1+2P)$.

Example 2: Assume there are M transmitters and M relays. Relay m wants to recover the message from transmitter m. This corresponds to setting the desired coefficient vector to be a unit vector $\mathbf{a}_m = \delta_m$. Substituting this choice into Theorem 4, we get that the messages can be decoded if their rates satisfy

$$R_m < \log^+ \left(\left(1 - \frac{P|h_{mm}|^2}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right) \tag{23}$$

$$= \log^+ \left(\left(\frac{1+P\sum_{\ell\neq m}|h_{m\ell}|^2}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right) \tag{24}$$

$$= \log \left(1 + \frac{P|h_{mm}|^2}{1+P\sum_{\ell\neq m}|h_{m\ell}|^2} \right) . \tag{25}$$

This is exactly the rate achievable with standard multiple-access techniques if the relays ignore all other messages as noise. In Section VII, we will use successive cancellation of lattice equations to show that if a relay wants all of the messages, any point in the Gaussian multiple-access rate region is achievable with compute-and-forward.

Remark 5: The setup in Example 2 is exactly that of an M-user Gaussian interference channel. Higher rates are possible by incorporating techniques such as the superposition of public and private messages [62], [63] and interference alignment [40], [41]. Note that these can be implemented in concert with compute-and-forward. For instance, in Section VIII, we describe a superposition compute-and-forward strategy.

In general, the choice of the coefficient vector $\mathbf{a}_m$ at each relay will depend both on the channel coefficients and the message demands at the destinations. Relays should make use of their available channel state information (CSI) to determine the most valuable equation to forward. One simple greedy approach is to choose coefficient vectors with the highest computation rate

$$\mathbf{a}_m = \arg\max_{\tilde{\mathbf{a}}} \mathcal{R}(\mathbf{h}_m, \tilde{\mathbf{a}}) \ . \tag{26}$$

This is a compelling strategy for scenarios where only local CSI is available. It resembles random linear network coding [27] except here the randomness stems entirely from the channel coefficients. In the next lemma, we demonstrate that this maximization does not require a search over all integer vectors.

Lemma 1: For a given channel vector $\mathbf{h}$, the computation rate $\mathcal{R}(\mathbf{h}_m, \mathbf{a}_m)$ from Theorems 2 and 4 are zero if the coefficient vector $\mathbf{a}$ satisfies:

$$\|\mathbf{a}_m\|^2 \geq 1 + \|\mathbf{h}_m\|^2 P. \tag{27}$$

Proof: Note that $|\mathbf{h}_m^* \mathbf{a}_m|^2 \leq \|\mathbf{h}_m\|^2 \|\mathbf{a}_m\|^2$ by the Cauchy-Schwarz inequality. Using this, we can upper bound the computation rate:

$$\log^+ \left(\left(\|\mathbf{a}_m\|^2 - \frac{P\ |\mathbf{h}_m^* \mathbf{a}_m|^2}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right) \tag{28}$$

$$\begin{aligned} &= \log^+ \left(\frac{1+P\|\mathbf{h}_m\|^2}{\|\mathbf{a}_m\|^2 + P\|\mathbf{h}_m\|^2\|\mathbf{a}_m\|^2 - P\ |\mathbf{h}_m^* \mathbf{a}_m|^2} \right) \\ &\leq \log^+ \left(\frac{1+P\|\mathbf{h}_m\|^2}{\|\mathbf{a}_m\|^2} \right) . \end{aligned} \tag{29}$$

The result follows immediately. ∎

In Figure 3, we have plotted how the computation rate from Theorem 2 varies as the channel coefficients change for several possible coefficients vectors. In this example, the message rates are symmetric $R_1 = R_2 = R$ and the power is 10dB. The channel vector $\mathbf{h} = [h\ 1]^T$ is parametrized by h which is varied between 0 and 2. The coefficient vectors are $\mathbf{a} = [1\ 0]^T$, $[1\ 1]^T$, and $[2\ 1]^T$. Each of these vectors attain its maximum computation rate when the channel vector is an exact match.

Remark 6: As the power increases, more coefficient vectors should be used to approximate the channel more finely. However, in the high SNR limit, it has recently been shown by Niesen and Whiting that the degrees-of-freedom (DoF) of our scheme becomes discontinuous [64]. Specifically, at rational channel vectors, our scheme attains the maximum DoF but, at irrational vectors, the DoF is upper bounded by a constant as the number of users increases. Under the assumption that the transmitters know the channel realization, they can attain

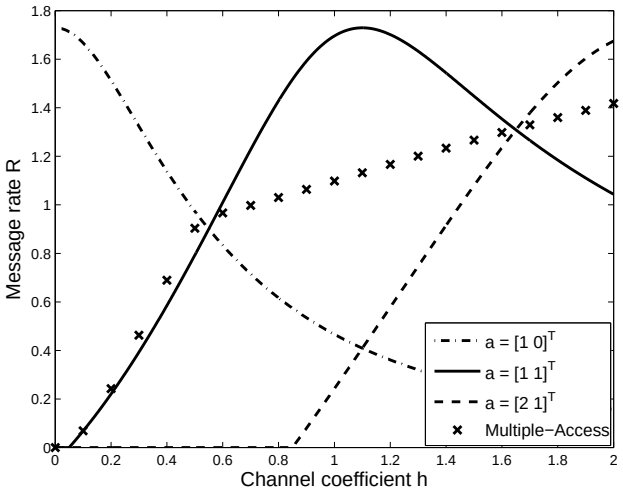

Fig. 3. Recovering equations with coefficient vectors $\mathbf{a} = [1\ 0]^T, [1\ 1]^T, [2\ 1]^T$ over a multiple-access channel with channel vector $\mathbf{h} = [h\ 1]$ where h varies between 0 and 2. The message rates are symmetric $R_1 = R_2 = R$ and the power is $P = 10$dB. For comparison, we have also plotted the symmetric multiple-access capacity.

the maximum DoF (up to a set of measure zero) by coupling compute-and-forward with the interference alignment scheme of Motahari *et al.* for fixed channels [65].

Remark 7: Note that each relay is free to decode more than one equation, so long as all the appropriate computation rates are satisfied. In some cases, it may be beneficial to recover a desired equation by first decoding equations of subsets of messages and then combining them.

The following example shows that it is useful to allow for a different rate at each transmitter.

Example 3: Consider a complex-valued AWGN network with $L = 4$ transmitters and $M = 2$ relays. The channel vectors are $\mathbf{h}_1 = [4\ -4\ \ 1\ -1]^T$ and $\mathbf{h}_2 = [1\ \ 1\ \ 2\ \ 2]^T$. The desired coefficient vectors are $\mathbf{a}_1 = \mathbf{h}_1$ and $\mathbf{a}_2 = [0\ \ 0\ \ 1\ \ 1]^T$. These equations can be reliably recovered so long as the message rates satisfy:

$$R_\ell < \begin{cases} \log^+\left(\frac{1}{34} + P\right) & \ell = 1, 2 \\ \log^+\left(\frac{1}{2} + \frac{4P}{1+2P}\right) & \ell = 3, 4 \end{cases} \tag{30}$$

IV. Nested Lattice Codes

In order to allow relays to decode integer combinations of codewords, we need codebooks with a linear structure. Specifically, we will use nested lattice codes that have both good statistical and good algebraic properties. Erez and Zamir developed a class of nested lattice codes that can approach the capacity of point-to-point AWGN channels in [15]. These codes operate under a modulo arithmetic that is well-suited for mapping operations over a finite field to the complex field.

First, we will provide some necessary definitions from [15] on nested lattice codes. Note that all of these definitions are given over $\mathbb{R}^n$. For complex-valued channels, our scheme will use the same lattice code over the real and imaginary parts of the channel input (albeit with different messages).

A. Lattice Definitions

Definition 12 (Lattice): An n-dimensional *lattice*, Λ, is a set of points in $\mathbb{R}^n$ such that if $\mathbf{s}, \mathbf{t} \in \Lambda$, then $\mathbf{s} + \mathbf{t} \in \Lambda$, and if $\mathbf{s} \in \Lambda$, then $-\mathbf{s} \in \Lambda$. A lattice can always be written in terms of a lattice generator matrix $\mathbf{B} \in \mathbb{R}^{n \times n}$:

$$\Lambda = \{\mathbf{s} = \mathbf{B}\mathbf{c} : \mathbf{c} \in \mathbb{Z}^n\} \ . \tag{31}$$

Definition 13 (Nested Lattices): A lattice Λ is said to be *nested* in a lattice Λ_1 if $\Lambda \subseteq \Lambda_1$. We will sometimes refer to Λ as the coarse lattice and Λ_1 as the fine lattice. More generally, a sequence of lattices $\Lambda, \Lambda_1, \ldots, \Lambda_L$ is nested if $\Lambda \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_L$.

Definition 14 (Quantizer): A *lattice quantizer* is a map, $Q_\Lambda : \mathbb{R}^n \to \Lambda$, that sends a point, $\mathbf{s}$, to the nearest lattice point in Euclidean distance:

$$Q_\Lambda(\mathbf{s}) = \arg\min_{\lambda \in \Lambda} ||\mathbf{s} - \lambda|| \ . \tag{32}$$

Definition 15 (Voronoi Region): The *fundamental Voronoi region*, $\mathcal{V}$, of a lattice, is the set of all points in $\mathbb{R}^n$ that are closest to the zero vector: $\mathcal{V} = \{\mathbf{s} : Q_\Lambda(\mathbf{s}) = \mathbf{0}\}$. Let $\mathsf{Vol}(\mathcal{V})$ denote the volume of $\mathcal{V}$.

Definition 16 (Modulus): Let $[\mathbf{s}] \bmod \Lambda$ denote the quantization error of $\mathbf{s} \in \mathbb{R}^n$ with respect to the lattice Λ,

$$[\mathbf{s}] \bmod \Lambda = \mathbf{s} - Q_\Lambda(\mathbf{s}) \ . \tag{33}$$

For all $\mathbf{s}, \mathbf{t} \in \mathbb{R}^n$ and $\Lambda \subseteq \Lambda_1$, the $\bmod \Lambda$ operation satisfies:

$$[\mathbf{s} + \mathbf{t}] \bmod \Lambda = \big[[\mathbf{s}] \bmod \Lambda + \mathbf{t}\big] \bmod \Lambda \tag{34}$$

$$\big[Q_{\Lambda_1}(\mathbf{s})\big] \bmod \Lambda = \big[Q_{\Lambda_1}\big([\mathbf{s}] \bmod \Lambda\big)\big] \bmod \Lambda \tag{35}$$

$$[a\mathbf{s}] \bmod \Lambda = [a[\mathbf{s}] \bmod \Lambda] \bmod \Lambda \qquad \forall a \in \mathbb{Z} \tag{36}$$

$$\beta[\mathbf{s}] \bmod \Lambda = [\beta\mathbf{s}] \bmod \beta\Lambda \qquad \forall \beta \in \mathbb{R} \tag{37}$$

Definition 17 (Nested Lattice Codes): A *nested lattice code* $\mathcal{L}$ is the set of all points of a fine lattice Λ_1 that are within the fundamental Voronoi region $\mathcal{V}$ of a coarse lattice Λ,

$$\mathcal{L} = \Lambda_1 \cap \mathcal{V} = \{\mathbf{t} : \mathbf{t} = \lambda \bmod \Lambda, \lambda \in \Lambda_1\} \ . \tag{38}$$

The rate of a nested lattice code is

$$r = \frac{1}{n} \log |\mathcal{L}| = \frac{1}{n} \log \frac{\mathsf{Vol}(\mathcal{V})}{\mathsf{Vol}(\mathcal{V}_1)} \ . \tag{39}$$

Let $\mathcal{B}(r)$ denote an n-dimensional ball of radius r,

$$\mathcal{B}(r) \triangleq \{\mathbf{s} : \|\mathbf{s}\| \le r,\ \mathbf{s} \in \mathbb{R}^n\} \tag{40}$$

and let $\mathrm{Vol}(\mathcal{B}(r))$ denote its volume.

Definition 18 (Covering Radius): The *covering radius* of a lattice Λ is the smallest real number r_{COV} such that $\mathbb{R}^n \subseteq \Lambda + \mathcal{B}(r_{\text{COV}})$.

Definition 19 (Effective Radius): The *effective radius* of a lattice with Voronoi region $\mathcal{V}$ is the real number r_{EFFEC} that satisfies $\mathsf{Vol}(\mathcal{B}(r_{\text{EFFEC}})) = \mathsf{Vol}(\mathcal{V})$.

Definition 20 (Moments): The *second moment* of a lattice Λ is defined as the second moment per dimension of a uniform distribution over the fundamental Voronoi region $\mathcal{V}$,

$$\sigma^2_\Lambda = \frac{1}{n\mathsf{Vol}(\mathcal{V})} \int_{\mathcal{V}} \|\mathbf{x}\|^2 d\mathbf{x} \ . \tag{41}$$

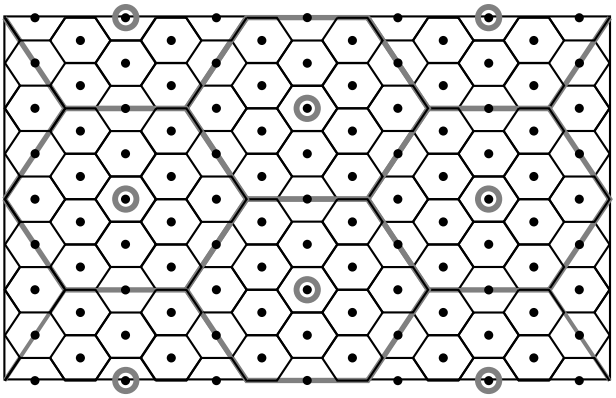

Fig. 4. Part of a nested lattice $\Lambda \subset \Lambda_1 \subset \mathbb{R}^2$. Black points are elements of the fine lattice Λ_1 and gray circles are elements of the coarse lattice Λ. The Voronoi regions for the fine and coarse lattice are drawn in black and gray respectively. A nested lattice code is the set of all fine lattice points within the Voronoi region of the coarse lattice centered on the origin.

The *normalized second moment* of a lattice is given by

$$G(\Lambda) = \frac{\sigma_\Lambda^2}{(\mathsf{Vol}(\mathcal{V}))^{2/n}} \ . \tag{42}$$

The following three definitions are the basis for proving AWGN channel coding theorems using nested lattice codes. Let $\Lambda^{(n)}$ denote a sequence of lattices indexed by their dimension.

Definition 21 (Covering Goodness): A sequence of lattices $\Lambda^{(n)} \subset \mathbb{R}^n$ is *good for covering* if

$$\lim_{n\to\infty} \frac{r_{\text{COV}}^{(n)}}{r_{\text{EFFEC}}^{(n)}} = 1 \ . \tag{43}$$

Such lattices were shown to exist by Rogers [66].

Definition 22 (Quantization Goodness): A sequence of lattices $\Lambda^{(n)} \subset \mathbb{R}^n$ is *good for mean-squared error (MSE) quantization* if

$$\lim_{n\to\infty} G(\Lambda^{(n)}) = \frac{1}{2\pi e} \ . \tag{44}$$

Zamir, Feder, and Poltyrev showed that sequences of such lattices exist in [67].

Definition 23 (AWGN Goodness): Let $\mathbf{z}$ be a length-n i.i.d. Gaussian vector, $\mathbf{z} \sim \mathcal{N}(0, \sigma_Z^2 \mathbf{I}^{n\times n})$. The volume-to-noise ratio of a lattice is given by

$$\mu(\Lambda, \epsilon) = \frac{(\mathsf{Vol}(\mathcal{V}))^{2/n}}{\sigma_Z^2} \tag{45}$$

where σ_Z^2 is chosen such that $\Pr\{\mathbf{z} \notin \mathcal{V}\} = \epsilon$. A sequence of lattices $\Lambda^{(n)}$ is *good for AWGN* if

$$\lim_{n\to\infty} \mu(\Lambda^{(n)}, \epsilon) = 2\pi e \quad \forall \epsilon \in (0,1) \tag{46}$$

and, for fixed volume-to-noise ratio greater than $2\pi e$, $\Pr\{\mathbf{z} \notin \mathcal{V}^{(n)}\}$ decays exponentially in n. In [68], Poltyrev demonstrated the existence of such lattices.

B. Lattice Constructions

Our nested lattice codes are a slight variant of those used by Erez and Zamir to approach the capacity of a point-to-point AWGN channel [15]. As in their considerations, we will have a coarse lattice that is good for covering, quantization, and AWGN and a fine lattice that is good for AWGN. We generalize this construction to include multiple nested fine lattices all of which are good for AWGN. This will allow each transmitter to operate at a different rate.

Lemma 2 (Erez-Litsyn-Zamir): There exists a sequence of lattices $\Lambda^{(n)}$ that is simultaneously good for covering, quantization, and AWGN.

This is a corollary of their main result which develops lattices that are good in all the above senses as well as for packing [69, Theorem 5]. Note that these lattices are built using Construction A which is described below.

We will use a coarse lattice Λ of dimension n from Lemma 2 scaled such that its second moment is equal to P. Let $\mathbf{B} \in \mathbb{R}^{n\times n}$ denote the generator matrix of this lattice. Our fine lattices are defined using the following procedure (the first three steps of which are often referred to as Construction A [69], [70]):

1) Draw a matrix $\mathbf{G}_L \in \mathbb{F}_p^{n\times k_L}$ with every element chosen i.i.d. according to the uniform distribution over $\{0, 1, 2, \ldots, p-1\}$. Recall that p is prime.
2) Define the codebook $\mathcal{C}_L$ as follows:

$$\mathcal{C}_L = \left\{\mathbf{c} = \mathbf{G}_L\mathbf{w} : \mathbf{w} \in \mathbb{F}_p^{k_L}\right\}. \tag{47}$$

   All operations in this step are over $\mathbb{F}_p$.
3) Form the lattice $\tilde{\Lambda}_L$ by projecting the codebook into the reals by $g(\cdot)$, scaling down by a factor of p, and placing a copy at every integer vector. This tiles the codebook over $\mathbb{R}^n$,

$$\tilde{\Lambda}_L = p^{-1} g(\mathcal{C}_L) + \mathbb{Z}^n \ . \tag{48}$$

4) Rotate $\tilde{\Lambda}_L$ by the generator matrix of the coarse nested lattice to get the fine lattice for transmitter L,

$$\Lambda_L = \mathbf{B}\tilde{\Lambda}_L \ . \tag{49}$$

5) Repeat steps 1) - 4) for each transmitter $\ell = 1, 2, \ldots, L-1$ by replacing $\mathbf{G}_L$ with $\mathbf{G}_\ell$ which is defined to be the first k_ℓ columns of $\mathbf{G}_L$.

Recall that $k_1 \geq \cdots \geq k_L$. Any pair of fine lattices $\Lambda_{\ell_1}, \Lambda_{\ell_2}, 1 \leq \ell_1 < \ell_2 < L$ are nested since all elements of $\mathcal{C}_{\ell_1}$ can be found from $\mathbf{G}_{\ell_2}$ by multiplying by all $\mathbf{w} \in \mathbb{F}^{n\times k_{\ell_2}}$ with zeros in the last $\ell_2 - \ell_1$ elements. Also observe that $\Lambda = \mathbf{B}\mathbb{Z}^n$ is nested within each fine lattice by construction. Therefore, the lattices are nested in the desired order, $\Lambda \subseteq \Lambda_L \subseteq \cdots \subseteq \Lambda_1$.

We now enforce that all the underlying generator matrices $\mathbf{G}_\ell$ are full rank. By the union bound, we get that:

$$\Pr\left(\bigcup_{\ell=1}^{L}\{\mathsf{rank}(\mathbf{G}_\ell)<k_\ell\}\right)\le\sum_{\ell=1}^{L}\sum_{\substack{\mathbf{w}\in\mathbb{F}_p^{k_\ell}\\ \mathbf{w}\neq\mathbf{0}}}\Pr\{\mathbf{G}_\ell\mathbf{w}=\mathbf{0}\}$$
$$=p^{-n}\sum_{\ell=1}^{L}(p^{k_\ell}-1) \qquad (50)$$

Thus, by choosing p and $k_1,\ldots,k_L$ to grow appropriately with n, all matrices $\mathbf{G}_1,\ldots,\mathbf{G}_L$ are full rank with probability that goes to 1 with n. Note that if $\mathbf{G}_\ell$ has full rank, then the number of fine lattice points in the fundamental Voronoi region $\mathcal{V}$ of the coarse lattice is given by $|\Lambda_\ell\cap\mathcal{V}|=p^{k_\ell}$ so that the rate of the ℓ^{th} nested lattice code $\mathcal{L}_\ell=\Lambda_\ell\cap\mathcal{V}$ is

$$r_\ell=\frac{1}{n}\log|\Lambda_\ell\cap\mathcal{V}|=\frac{k_\ell}{n}\log p=R_\ell \qquad (51)$$

as desired. (In the complex-valued case, we set $r_\ell=R_\ell/2$.) In Appendix B, we show that the fine lattices are AWGN good so long as $\frac{n}{p}\to 0$ as n grows. There are many choices of p and $k_1,\ldots,k_L$ that will ensure that the fine lattices have the desired properties. One possibility is to let p grow like $n\log n$ and set $k_\ell=\lfloor nR_\ell(\log p)^{-1}\rfloor$.

Remark 8: We require that the fine lattices are generated from full-rank submatrices of the same finite field codebook so that it is possible to compute linear equations over messages with different rates. The full rank condition on the coarse lattice allows us to move between lattice equations and equations of finite field messages.

In [69], [71], some useful properties of nested lattices derived from Construction A are established. These apply to our construction as well and we repeat them below.

Lemma 3: Let $\Lambda_\ell(i)$ denote the i^{th} point in the ℓ^{th} nested lattice code $\mathcal{L}_\ell=\Lambda_\ell\cap\mathcal{V}$ for $i=0,1,2,\ldots,p^{k_\ell}-1$ from the random lattice construction above. We have that:

- $\Lambda_\ell(i)$ is uniformly distributed over $p^{-1}\Lambda\cap\mathcal{V}$.
- For any $i_1\neq i_2,\ [\Lambda_\ell(i_1)-\Lambda_\ell(i_2)] \bmod \Lambda$ is uniformly distributed over $\{p^{-1}\Lambda\}\cap\mathcal{V}$.

Thus, each fine lattice can be interpreted as a diluted version of a scaled down coarse lattice $p^{-1}\Lambda$.

C. Integer Combinations of Lattice Points

Our scheme relies on mapping messages from a finite field to codewords from a nested lattice code. The relay will first decode an integer combination of lattice codewords and then convert this into an equation of the messages.

Definition 24 (Lattice Equation): A *lattice equation* $\mathbf{v}$ is an integer combination of lattice codewords $\mathbf{t}_\ell\in\mathcal{L}_\ell$ modulo the coarse lattice,

$$\mathbf{v}=\left[\sum_{\ell=1}^{L}a_\ell\mathbf{t}_\ell\right] \bmod \Lambda \qquad (52)$$

for some coefficients $a_\ell\in\mathbb{Z}$.

Note that the lattice equation takes values on the finest lattice in the summation. That is, if $a_1,\ldots,a_{\ell-1}=0$ then the lattice equation $\mathbf{v}$ only takes values on $\mathcal{L}_\ell=\Lambda_\ell\cap\mathcal{V}$.

Lemma 4: Any lattice Λ that results from Construction A has a full-rank generator matrix $\mathbf{B}$.

Proof: Note that $\mathbb{Z}^n\subset\Lambda$ so that Λ contains all of the unit vectors by default. Thus, $\mathbf{B}$ spans $\mathbb{R}^n$ and is full rank. ■

Since our nested lattice codes are built using nested finite field codes, it is possible to map messages to lattice points and back while preserving linearity. The next two lemmas make this notion precise.

Lemma 5: Let $\mathbf{w}_\ell$ be a message in $\mathbb{F}_p^{k_\ell}$ that is zero-padded to length k. The function

$$\phi(\mathbf{w}_\ell)=\left[\mathbf{L}p^{-1}g(\mathbf{G}\mathbf{w}_\ell)\right] \bmod \Lambda \qquad (53)$$

is a one-to-one map between the set of such messages and the elements of the nested lattice code $\mathcal{L}_\ell=\Lambda_\ell\cap\mathcal{V}$.

Proof: Since the last $k-k_\ell$ elements of $\mathbf{w}_\ell$ are zero, multiplying the message by $\mathbf{G}$ is the same as multiplying the first k_ℓ elements by $\mathbf{G}_\ell$. Since $\mathbf{G}_\ell$ is assumed to be full rank, it takes $\mathbf{w}_\ell$ to a unique point in the finite field codebook $\mathcal{C}_\ell$. The function g simply maps finite field elements to integers and p^{-1} is a rescaling so $p^{-1}g(\mathbf{G}\mathbf{w}_\ell)$ maps $\mathbf{w}_\ell$ to a unique point in $[0,1)^n$. Lemma 4 shows that $\mathbf{B}$ is full rank so we just need show that the $\bmod\Lambda$ operation is a bijection between $\mathbf{B}[0,1)^n$ and $\mathcal{V}$. Assume, for the sake of a contradiction, $\exists x,y\in\mathbf{B}[0,1)^n, x\neq y$ such that $[x] \bmod\Lambda=[y] \bmod\Lambda$. This implies that $x-Q_\Lambda(x)=y-Q_\Lambda(y)$. Now multiply both sides by $\mathbf{B}^{-1}$ and then take the modulus with respect to $\mathbb{Z}^n$,

$$[\mathbf{B}^{-1}(x-Q_\Lambda(x))] \bmod \mathbb{Z}^n=[\mathbf{B}^{-1}(y-Q_\Lambda(y))] \bmod \mathbb{Z}^n$$
$$[\mathbf{B}^{-1}x] \bmod \mathbb{Z}^n=[\mathbf{B}^{-1}y] \bmod \mathbb{Z}^n$$
$$x=y$$

where the second line follows since for any $\lambda\in\Lambda,\ \mathbf{B}^{-1}\lambda\in\mathbb{Z}^n$. A contradiction has been reached which shows that $\bmod\Lambda$ is a bijection. Combining this with the fact that the finite field and the nested lattice code have the same number of elements, $|\mathbb{F}_p^{k_\ell}|=|\Lambda_\ell\cap\mathcal{V}|=p^{k_\ell}$, shows that ϕ_ℓ is a one-to-one map. ■

Lemma 6: Let $\mathbf{u}=\bigoplus_\ell q_\ell\mathbf{w}_\ell$ be the desired equation for some coefficients $q_\ell\in\mathbb{F}_p$ and messages $\mathbf{w}_\ell\in\mathbb{F}_p^{k_\ell}$ zero-padded to length k. Assume the messages are mapped to nested lattice codewords, $\mathbf{t}_\ell=\phi(\mathbf{w}_\ell)$, and let $\mathbf{v}=[\sum a_\ell\mathbf{t}_\ell] \bmod\Lambda$ denote the lattice equation for some $a_\ell\in\mathbb{Z}$ such that $q_\ell=g^{-1}([a_\ell] \bmod p)$. Then the desired equation can be obtained using $\mathbf{u}=\phi^{-1}(\mathbf{v})$ where

$$\phi^{-1}(\mathbf{v})=(\mathbf{G}^T\mathbf{G})^{-1}\mathbf{G}^Tg^{-1}\left(p[\mathbf{B}^{-1}\mathbf{v}] \bmod \mathbb{Z}^n\right). \qquad (54)$$

Proof: Recall that since $\mathbf{B}$ is the generator matrix of Λ, $\mathbf{B}^{-1}\Lambda=\mathbb{Z}^n$. Also note that since $\mathbf{w}_\ell$ is zero-padded to length k, then multiplying by $\mathbf{G}$ has the same effect as multiplying

the original message by $\mathbf{G}_\ell$. We have that

$$[\mathbf{B}^{-1}\mathbf{v}] \bmod \mathbb{Z}^n \tag{55}$$

$$= \left[\mathbf{B}^{-1}\sum_{\ell=1}^{L} a_\ell \mathbf{t}_\ell - \mathbf{B}^{-1}Q_\Lambda\left(\sum_{\ell=1}^{L} a_\ell \mathbf{t}_\ell\right)\right] \bmod \mathbb{Z}^n \tag{56}$$

$$\overset{\text{(a)}}{=} \left[\mathbf{B}^{-1}\sum_{\ell=1}^{L} a_\ell \mathbf{t}_\ell\right] \bmod \mathbb{Z}^n \tag{57}$$

$$\overset{\text{(b)}}{=} \left[\sum_{\ell=1}^{L} a_\ell\Big(p^{-1}g(\mathbf{G}\mathbf{w}_\ell) - \mathbf{B}^{-1}Q_\Lambda\Big(\mathbf{B}p^{-1}g(\mathbf{G}\mathbf{w}_\ell)\Big)\Big)\right] \bmod \mathbb{Z}^n \tag{58}$$

$$\overset{\text{(c)}}{=} \left[\sum_{\ell=1}^{L} a_\ell p^{-1}g(\mathbf{G}\mathbf{w}_\ell)\right] \bmod \mathbb{Z}^n \tag{59}$$

where (a) and (c) follow since $Q_\Lambda(\cdot)$ is an element of Λ so $\mathbf{B}^{-1}Q_\Lambda(\cdot)$ is an element of $\mathbb{Z}^n$ and (b) follows using (53). Multiplying by p and applying (37) yields

$$p[\mathbf{B}^{-1}\mathbf{v}] \bmod \mathbb{Z}^n = \left[\sum_{\ell=1}^{L} a_\ell g(\mathbf{G}\mathbf{w}_\ell)\right] \bmod p\mathbb{Z}^n \tag{60}$$

$$\overset{\text{(d)}}{=} \left[g\left(\bigoplus_{\ell=1}^{L} q_\ell \mathbf{G}\mathbf{w}_\ell\right)\right] \bmod p\mathbb{Z}^n \tag{61}$$

$$= g\left(\bigoplus_{\ell=1}^{L} q_\ell \mathbf{G}\mathbf{w}_\ell\right) \tag{62}$$

where (d) follows since g maps between $\{0,1,\ldots,p-1\}$ and $\mathbb{F}_p$ and $q_\ell = g^{-1}([a] \bmod p)$.
Applying g^{-1} to move back to the finite field we get

$$g^{-1}\left(p[\mathbf{B}^{-1}\mathbf{v}] \bmod \mathbb{Z}^n\right) = \mathbf{G}\bigoplus_{\ell=1}^{L} q_\ell \mathbf{w}_\ell \tag{63}$$

Finally, note that $\left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T$ is the left-inverse of $\mathbf{G}$ which implies that $\phi^{-1}(\mathbf{v}) = \mathbf{u}$. ∎

V. Compute-and-Forward

In this section, we provide a detailed description of our coding scheme. See Figure 5 for a block diagram. The following four steps are a basic outline:

1) Each transmitter maps its message from the finite field onto an element of a nested lattice code.
2) The lattice codewords are transmitted over the channel.
3) Each relay decodes a linear equation of the lattice codewords.
4) These lattice equations are mapped back to the finite field to get the desired linear combination of messages.

We begin with the proof for the real-valued case and then move on to the complex-valued case.

A. Real-Valued Channel Models

When a relay attempts to decode an integer combination of the lattice points, it must overcome two sources of noise. One is simply the channel noise $\mathbf{z}$. The other is due to the fact that the channel coefficients that are often not exactly equal to the desired equation coefficients. As a result, part of the noise stems from the codewords themselves (sometimes referred to as "self-noise"). To overcome this issue, the transmitters will dither their lattice points using common randomness that is also known to the relays. This dithering makes the transmitted codewords independent from the underlying lattice points. Since our scheme works with respect to expectation over these dither vectors, then it can be shown that (at least) one set of good fixed dither vectors exists (which means that no common randomness is actually necessary). We defer the proof of this fact to Appendix C. The following lemma from [15] captures a key property of dithered nested lattice codes.

Lemma 7 (Erez-Zamir): Let $\mathbf{t}$ be a random vector with an arbitrary distribution over $\mathbb{R}^n$. If $\mathbf{d}$ is independent of $\mathbf{t}$ and uniformly distributed over $\mathcal{V}$, then $[\mathbf{t}-\mathbf{d}] \bmod \Lambda$ is also independent of $\mathbf{t}$ and uniformly distributed over $\mathcal{V}$.

We now set out to prove that the relays can reliably recover integer combinations of transmitted lattice points.

Theorem 5: For any $\epsilon > 0$ and n large enough, there exist nested lattice codes $\Lambda \subseteq \Lambda_L \subseteq \cdots \subseteq \Lambda_1$ with rates $r_1,\ldots,r_L$, such that for all channel vectors $\mathbf{h}_1,\ldots,\mathbf{h}_M \in \mathbb{R}^L$ and coefficient vectors $\mathbf{a}_1,\ldots,\mathbf{a}_M \in \mathbb{Z}^L$, relay m can decode the lattice equation

$$\mathbf{v}_m = \left[\sum_{\ell=1}^{L} a_{m\ell}\mathbf{t}_\ell\right] \bmod \Lambda \tag{64}$$

of transmitted lattice points $\mathbf{t}_\ell \in \mathcal{L}_\ell$ with average probability of error ϵ so long as

$$r_\ell < \min_{m:a_{m\ell}\neq 0} \frac{1}{2}\log^+\left(\frac{P}{\alpha_m^2 + P\|\alpha_m\mathbf{h}_m - \mathbf{a}_m\|^2}\right)$$

for some choice of $\alpha_1,\ldots,\alpha_M \in \mathbb{R}$.

Proof: Each encoder is given a dither vector $\mathbf{d}_\ell$ which is generated independently according to a uniform distribution over $\mathcal{V}$. All dither vectors are made available to each relay. Encoder ℓ dithers its lattice point, takes $\bmod \Lambda$, and transmits the result:

$$\mathbf{x}_\ell = [\mathbf{t}_\ell - \mathbf{d}_\ell] \bmod \Lambda\ . \tag{65}$$

By Lemma 7, $\mathbf{x}_\ell$ is uniform over $\mathcal{V}$ so $E[\|\mathbf{x}_\ell\|^2] = nP$, where the expectation is taken over the dithers. In Appendix C, we argue that there exist fixed dithers that meet the power constraint set forth in (1).

The channel output at relay m is

$$\mathbf{y}_m = \sum_{\ell=1}^{L} h_{m\ell}\mathbf{x}_\ell + \mathbf{z}_m\ . \tag{66}$$

Recall that the transmitters are ordered by decreasing message rates. Let $\ell_{\text{MAX}}(m) = \max\{\ell : a_{m\ell} \neq 0\}$ denote the highest index value of the non-zero coefficients in $\mathbf{a}_m$. Also, let Q_m denote the lattice quantizer for the corresponding fine lattice $\Lambda_{\ell_{\text{MAX}}(m)}$. Note that this is the highest rate message in the equation and thus the rate of the equation itself. Each relay

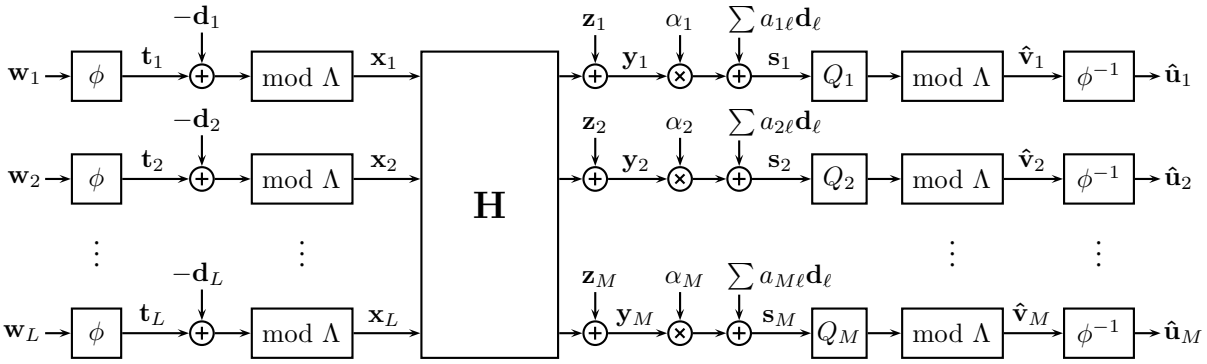

Fig. 5. System diagram of the nested lattice encoding and decoding operations employed as part of the compute-and-forward framework (for real-valued channel models). Each message $\mathbf{w}_\ell$ is mapped to a lattice codeword $\mathbf{t}_\ell$, dithered, and transmitted as $\mathbf{x}_\ell$. Each relay observes $\mathbf{y}_m$ which it scales by α_m. It then removes the dithers, quantizes the result onto the fine lattice using Q_m, and maps it onto the fundamental Voronoi region of the coarse lattice using $\bmod \Lambda$. Finally, the relay maps its estimate $\hat{\mathbf{v}}_m$ of the lattice equation $\mathbf{v}_m = [\sum a_{m\ell}\mathbf{t}_\ell] \bmod \Lambda$ back to the finite field using ϕ^{-1} to get an estimate $\hat{\mathbf{u}}_m$ of a linear equation of the messages $\mathbf{u}_m = \bigoplus q_{m\ell}\mathbf{w}_\ell$ where $q_{m\ell} = g^{-1}([a_{m\ell}] \bmod p)$ are the finite field representations of the coefficients.

computes

$$\mathbf{s}_m = \alpha_m \mathbf{y}_m + \sum_{\ell=1}^{L} a_{m\ell}\mathbf{d}_\ell \ . \tag{67}$$

To get an estimate of the lattice equation $\mathbf{v}_m$, this vector is quantized onto $\Lambda_{\ell_{\text{MAX}}(m)}$ modulo the coarse lattice Λ:

$$\hat{\mathbf{v}}_m = \big[Q_m(\mathbf{s}_m)\big] \bmod \Lambda \ . \tag{68}$$

Using (35), we get that

$$\big[Q_m(\mathbf{s}_m)\big] \bmod \Lambda = \big[Q_m([\mathbf{s}_m] \bmod \Lambda)\big] \bmod \Lambda \ . \tag{69}$$

We now show that $[\mathbf{s}_m] \bmod \Lambda$ is equivalent to $\mathbf{v}_m$ plus some noise terms. Let $\theta_{m\ell} = \alpha_m h_{m\ell} - a_{m\ell}$.

$$[\mathbf{s}_m] \bmod \Lambda \tag{70}$$

$$= \left[\sum_{\ell=1}^{L} \Big(\alpha_m h_{m\ell}\mathbf{x}_\ell + a_{m\ell}\mathbf{d}_\ell\Big) + \alpha_m \mathbf{z}_m\right] \bmod \Lambda \tag{71}$$

$$= \left[\sum_{\ell=1}^{L} \Big(a_{m\ell}(\mathbf{x}_\ell + \mathbf{d}_\ell) + \theta_{m\ell}\mathbf{x}_\ell\Big) + \alpha_m \mathbf{z}_m\right] \bmod \Lambda \tag{72}$$

$$= \left[\sum_{\ell=1}^{L} a_{m\ell}\Big([\mathbf{t}_\ell - \mathbf{d}_\ell] \bmod \Lambda + \mathbf{d}_\ell\Big) + \sum_{\ell=1}^{L} \theta_{m\ell}\mathbf{x}_\ell + \alpha_m \mathbf{z}_m\right] \bmod \Lambda \tag{73}$$

$$= \left[\sum_{\ell=1}^{L} a_{m\ell}\mathbf{t}_\ell + \sum_{\ell=1}^{L} \theta_{m\ell}\mathbf{x}_\ell + \alpha_m \mathbf{z}_m\right] \bmod \Lambda \tag{74}$$

$$= \left[\mathbf{v}_m + \sum_{\ell=1}^{L} \theta_{m\ell}\mathbf{x}_\ell + \alpha_m \mathbf{z}_m\right] \bmod \Lambda \tag{75}$$

where the last two steps are due to (34). From Lemma 7, the pair of random variables $(\mathbf{v}_m, \hat{\mathbf{v}}_m)$ has the same joint distribution as the pair $(\mathbf{v}_m, \tilde{\mathbf{v}}_m)$ defined by the following:

$$\tilde{\mathbf{v}}_m = \big[Q_m(\mathbf{v}_m + \mathbf{z}_{eq,m})\big] \bmod \Lambda \tag{76}$$

$$\mathbf{z}_{eq,m} = \alpha_m \mathbf{z}_m + \sum_{\ell=1}^{L} \theta_{m\ell}\tilde{\mathbf{d}}_\ell \tag{77}$$

where each $\tilde{\mathbf{d}}_\ell$ is drawn independently according to a uniform distribution over $\mathcal{V}$. See Figure 6 for a block diagram of the equivalent channel. The probability of error $\Pr(\hat{\mathbf{v}}_m \neq \mathbf{v}_m)$ is thus equal to the probability that the equivalent noise leaves the Voronoi region surrounding the codeword, $\Pr\big(\mathbf{z}_{m,eq} \notin \mathcal{V}_{\ell_{\text{MAX}}(m)}\big)$.

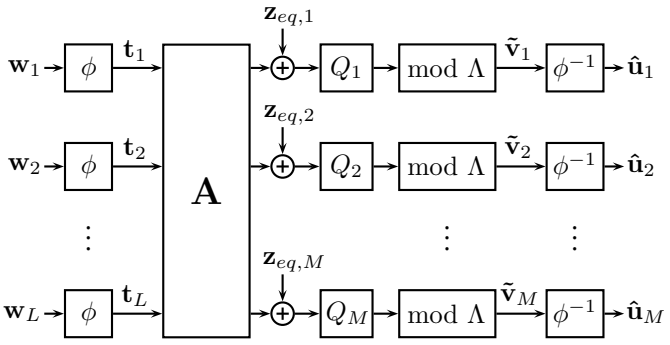

Fig. 6. Equivalent channel induced by the modulo-Λ transformation. In this "virtual" channel model, each encoder maps its message $\mathbf{w}_\ell$ to a lattice point $\mathbf{t}_\ell$. Each relay observes an integer combination $\sum a_{m\ell}\mathbf{t}_\ell$ of the lattice points corrupted by effective noise $\mathbf{z}_{eq,m}$. It then quantizes onto the fine lattice using Q_m and takes $\bmod \Lambda$ to get an estimate $\tilde{\mathbf{v}}_m$ of the lattice equation $\mathbf{v}_m = [\sum a_{m\ell}\mathbf{t}_\ell] \bmod \Lambda$. Finally, the relay maps the recovered lattice equation to an estimate $\hat{\mathbf{u}}_m$ of its desired linear equation of the messages $\mathbf{u}_m = \bigoplus q_{m\ell}\mathbf{w}_\ell$ where $q_{m\ell} = g^{-1}([a_{m\ell}] \bmod p)$ are the finite field representations of the coefficients.

Using Lemma 8 from Appendix A, the density of $\mathbf{z}_{eq,m}$ can be upper bounded (times a constant) by the density of an i.i.d. zero-mean Gaussian vector $\mathbf{z}_m^*$ whose variance σ_m^2 approaches

$$N_{eq,m} = \alpha_m^2 + P\sum_{\ell=1}^{L} \theta_{m\ell}^2 \tag{78}$$

$$= \alpha_m^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2 \tag{79}$$

as $n \to \infty$. We also show in Appendix B that $\Lambda_1, \Lambda_2, \ldots, \Lambda_L$ are good for AWGN. From Definition 23, this means that $\epsilon_m = \Pr(\mathbf{z}_m^* \notin \mathcal{V}_{\ell_{\text{MAX}}(m)})$ goes to zero exponentially in n so long as the volume-to-noise ratio satisfies $\mu(\Lambda_{\ell_{\text{MAX}}(m)}, \epsilon_m) >$

$2\pi e$. If this occurs, then $\Pr(\mathbf{z}_{eq,m} \notin \mathcal{V}_{\ell_{\text{MAX}}(m)})$ goes to zero exponentially in n as well. Note that, by the union bound, the average probability of error ϵ is upper bounded by the sum

$$\epsilon \leq \sum_{m=1}^{M} \Pr(\mathbf{z}_{eq,m} \notin \mathcal{V}_{\ell_{\text{MAX}}(m)}) \ . \tag{80}$$

To ensure that the probability of error goes to zero for all desired equations[3], we get that the volume of $\mathcal{V}_{\ell_{\text{MAX}}(m)}$ must satisfy

$$2\pi e < \mu(\Lambda_{\ell_{\text{MAX}}(m)}, \epsilon_m) = \frac{(\mathsf{Vol}(\mathcal{V}_{\ell_{\text{MAX}}(m)}))^{2/n}}{\sigma_m^2} \tag{81}$$

for all relays with $a_{m\ell} \neq 0$. If we set the volume of each Voronoi region $\mathcal{V}_\ell$ as follows, the constraints are always met:

$$\mathsf{Vol}(\mathcal{V}_\ell) > \left(2\pi e \max_{m:a_{m\ell}\neq 0} \sigma_m^2\right)^{n/2} \tag{82}$$

Recall that the rate of a nested lattice code is

$$r_\ell = \frac{1}{n} \log\left(\frac{\mathsf{Vol}(\mathcal{V})}{\mathsf{Vol}(\mathcal{V}_\ell)}\right). \tag{83}$$

Using (42), we can solve for the volume of the fundamental Voronoi region of the coarse lattice:

$$\mathsf{Vol}(\mathcal{V}) = \left(\frac{P}{G(\Lambda)}\right)^{n/2} \tag{84}$$

It follows that we can achieve any rate less than

$$r_\ell < \min_{m:a_{m\ell}\neq 0} \frac{1}{2} \log^+\left(\frac{P}{G(\Lambda) 2\pi e \sigma_m^2}\right) \tag{85}$$

Choose $\delta > 0$. Since Λ is good for quantization, for n large enough, we have that $G(\Lambda)2\pi e < (1+\delta)$. We also know that σ_m^2 converges to $N_{eq,m}$ so for n large enough we have $\sigma_m^2 < (1+\delta)N_{eq,m}$. Finally, we get that the rate r_ℓ of each nested lattice code is at least

$$\min_{m:a_{m\ell}\neq 0} \frac{1}{2} \log^+\left(\frac{P}{\alpha_m^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2}\right) - \log(1+\delta)$$

Thus, by choosing δ small enough, we can approach the computation rates as closely as desired. ∎

We now put all of these ingredients together to prove Theorem 1. See Figures 7 and 8 for block diagrams of the encoding and decoding process.

Proof of Theorem 1: See Figure 5 for a block diagram. Choose $\epsilon > 0$. Encoder ℓ maps its finite field message vector $\mathbf{w}_\ell$ to a lattice point $\mathbf{t}_\ell \in \Lambda_\ell \cap \mathcal{V}$, using ϕ from Lemma 5,

$$\mathbf{t}_\ell = \phi(\mathbf{w}_\ell) \ . \tag{86}$$

Using Theorem 5, these lattice points can be transmitted across the channel so that the relays can make estimates $\hat{\mathbf{v}}_m$ of lattice equations $\mathbf{v}_m$ with coefficient vectors $\mathbf{a}_m \in \mathbb{Z}^L$ such that $\Pr\left(\cup_m \{\hat{\mathbf{v}}_m \neq \mathbf{v}_m\}\right) < \epsilon$ for n large enough so long as

$$R_\ell < \min_{m:a_{m\ell}\neq 0} \frac{1}{2} \log^+\left(\frac{P}{\alpha_m^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2}\right)$$

[3]Note that by Lemma 1 the number of available coefficient vectors $\mathbf{a}_m$ at each relay is finite if $\|\mathbf{h}_m\|$ and P are finite. Therefore, it can be shown via a union bound that each relay can decode more than one equation.

for some $\alpha_1, \ldots, \alpha_M \in \mathbb{R}$. Finally, using ϕ^{-1} from Lemma 6, each relay can produce estimates of the desired linear combination of messages, $\hat{\mathbf{u}}_m = \phi^{-1}(\hat{\mathbf{v}}_m)$, such that $\Pr\left(\cup_m \{\hat{\mathbf{u}}_m \neq \mathbf{u}_m\}\right) < \epsilon$ where

$$\mathbf{u}_m = \bigoplus_{\ell=1}^{L} q_{m\ell} \mathbf{w}_\ell \tag{87}$$

$$q_{m\ell} = g^{-1}([a_{m\ell}] \bmod p) \ . \tag{88}$$

B. Complex-Valued Channel Models

We now show how to use nested lattice codes over complex-valued channel models.

Theorem 6: For any $\epsilon > 0$ and n large enough, there exist nested lattice codes $\Lambda \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_L$ with rates $R_1, \ldots, R_L$, such that for all channel vectors $\mathbf{h}_1, \ldots, \mathbf{h}_M \in \mathbb{R}^L$ and coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_M \in \{\mathbb{Z} + j\mathbb{Z}\}^L$, each relay can decode lattice equations $\mathbf{v}_m^R, \mathbf{v}_m^I$ where

$$\mathbf{v}_m^R = \left[\sum_{\ell=1}^{L} \mathsf{Re}(a_{m\ell})\mathbf{t}_\ell^R - \mathsf{Im}(a_{m\ell})\mathbf{t}_\ell^I\right] \bmod \Lambda \tag{89}$$

$$\mathbf{v}_m^I = \left[\sum_{\ell=1}^{L} \mathsf{Im}(a_{m\ell})\mathbf{t}_\ell^R + \mathsf{Re}(a_{m\ell})\mathbf{t}_\ell^I\right] \bmod \Lambda \tag{90}$$

of transmitted lattice points $\mathbf{t}_\ell^R, \mathbf{t}_\ell^I \in \Lambda_\ell \cap \mathcal{V}$ with average probability of error ϵ so long as

$$r_\ell < \frac{1}{2} \log^+\left(\frac{P}{|\alpha_m|^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2}\right) \tag{91}$$

for some choice of $\alpha_1, \ldots, \alpha_M \in \mathbb{C}$.

Proof: First, we scale our nested lattice ensemble so that the coarse lattice Λ has second moment $P/2$. Each encoder is given two dither vectors, $\mathbf{d}_\ell^R$ and $\mathbf{d}_\ell^I$, which are independently drawn according to a uniform distribution over $\mathcal{V}$. All dither vectors are made available to each relay. Encoder ℓ generates a channel input:

$$\mathbf{x}_\ell = \left[\mathbf{t}_\ell^R - \mathbf{d}_\ell^R\right] \bmod \Lambda + j\left[\mathbf{t}_\ell^I - \mathbf{d}_\ell^I\right] \bmod \Lambda \ . \tag{92}$$

By Lemma 7, the real and imaginary parts of $\mathbf{x}_\ell$ are independent and uniform over $\mathcal{V}$ so $E[\|\mathbf{x}_\ell\|^2] = nP$, with expectation taken over the dithers.[4]

Let $\ell_{\text{MAX}}(m) = \max\{\ell : a_{m\ell} \neq 0\}$ and let Q_m denote the lattice quantizer for $\Lambda_{\ell_{\text{MAX}}(m)}$. Each relay computes

$$\mathbf{s}_m^R = \mathsf{Re}(\alpha_m \mathbf{y}_m) + \sum_{\ell=1}^{L} \mathsf{Re}(a_{m\ell})\mathbf{d}_\ell^R - \mathsf{Im}(a_{m\ell})\mathbf{d}_\ell^I \tag{93}$$

$$\mathbf{s}_m^I = \mathsf{Im}(\alpha_m \mathbf{y}_m) + \sum_{\ell=1}^{L} \mathsf{Im}(a_{m\ell})\mathbf{d}_\ell^R + \mathsf{Re}(a_{m\ell})\mathbf{d}_\ell^I. \tag{94}$$

To get estimates of the lattice equations, these vectors are quantized onto $\Lambda_{\ell_{\text{MAX}}(m)}$ modulo the coarse lattice Λ:

$$\hat{\mathbf{v}}_m^R = \left[Q_m(\mathbf{s}_m^R)\right] \bmod \Lambda \tag{95}$$

$$\hat{\mathbf{v}}_m^I = \left[Q_m(\mathbf{s}_m^I)\right] \bmod \Lambda. \tag{96}$$

[4]In Appendix C, we argue that there exist fixed dithers that meet the power constraint $\|\mathbf{x}\|^2 \leq nP$.

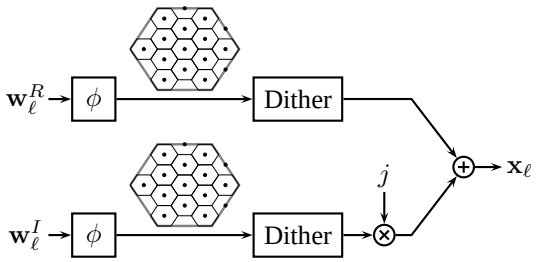

Fig. 7. Block diagram of the complex-valued compute-and-forward encoder at transmitter ℓ, $\mathcal{E}_\ell$. Messages from a finite field are mapped onto a nested lattice code, dithered, and transmitted across the channel.

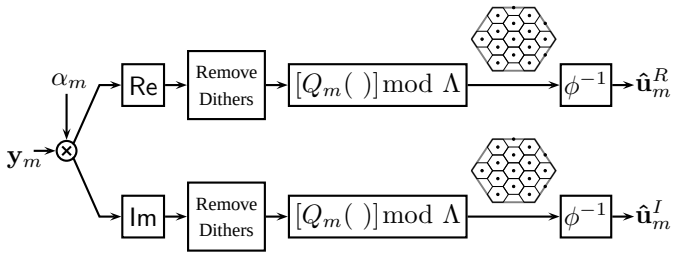

Fig. 8. Block diagram of the complex-valued compute-and-forward decoder for relay m, $\mathcal{D}_m$. The channel observation is scaled and decomposed into its real and imaginary components. The decoder then removes the dithers, quantizes onto the appropriate fine lattice, and takes the modulus over the coarse lattice. This results in an equation of lattice codewords which is then mapped into an equation of messages over the finite field.

Note that by (35) we have

$$\Big[Q_m\big(\mathbf{s}_m^R\big)\Big] \bmod \Lambda = \Big[Q_m\big(\big[\mathbf{s}_m^R\big] \bmod \Lambda\big)\Big] \bmod \Lambda. \quad (97)$$

Define $\theta_{m\ell}^R = \mathsf{Re}(\alpha_m h_{m\ell} - a_{m\ell})$ and $\theta_{m\ell}^I = \mathsf{Im}(\alpha_m h_{m\ell} - a_{m\ell})$. We now show that $[\mathbf{s}_m^R] \bmod \Lambda$ is equivalent to $\mathbf{v}_m^R$ plus some noise terms in (98)-(101). Using similar manipulations, it can be shown that $[\mathbf{s}_m^I] \bmod \Lambda$ is equivalent to $\mathbf{v}_m^I$ plus some noise terms as well. From Lemma 7, the pairs of random variables $(\mathbf{v}_m^R, \hat{\mathbf{v}}_m^R)$ and $(\mathbf{v}_m^I, \hat{\mathbf{v}}_m^I)$ have the same joint distributions as the pairs $(\mathbf{v}_m^R, \tilde{\mathbf{v}}_m^R)$ and $(\mathbf{v}_m^I, \tilde{\mathbf{v}}_m^I)$, respectively, where

$$\tilde{\mathbf{v}}_m^R = \big[Q_m(\mathbf{v}_m^R + \mathbf{z}_{eq,m}^R)\big] \bmod \Lambda \quad (102)$$

$$\tilde{\mathbf{v}}_m^I = \big[Q_m(\mathbf{v}_m^I + \mathbf{z}_{eq,m}^I)\big] \bmod \Lambda \quad (103)$$

$$\mathbf{z}_{eq,m}^R = \mathsf{Re}(\alpha_m \mathbf{z}_m) + \sum_{\ell=1}^{L} \theta_{m\ell}^R \tilde{\mathbf{d}}_\ell^R - \theta_{m\ell}^I \tilde{\mathbf{d}}_\ell^I \quad (104)$$

$$\mathbf{z}_{eq,m}^I = \mathsf{Im}(\alpha_m \mathbf{z}_m) + \sum_{\ell=1}^{L} \theta_{m\ell}^I \tilde{\mathbf{d}}_\ell^R + \theta_{m\ell}^R \tilde{\mathbf{d}}_\ell^I \quad (105)$$

where each $\tilde{\mathbf{d}}_\ell^R$ and $\tilde{\mathbf{d}}_\ell^I$ is drawn independently according to a uniform distribution over $\mathcal{V}$. Using Lemma 8 from Appendix A, we have that the densities of both $\mathbf{z}_{eq,m}^R$ and $\mathbf{z}_{eq,m}^I$ are upper bounded (times a constant) by the density of an i.i.d. zero-mean Gaussian vector $\mathbf{z}_m^*$ whose variance σ_m^2 approaches

$$N_{eq,m} = \frac{|\alpha_m|^2}{2} + \frac{P}{2}\Big(\big(\theta_{m\ell}^R\big)^2 + \big(\theta_{m\ell}^I\big)^2\Big) \quad (106)$$

$$= \frac{|\alpha_m|^2}{2} + \frac{P}{2}\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2 \quad (107)$$

as $n \to \infty$. Note that the effective SNR for both real and imaginary components is $P/(|\alpha_m|^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2)$ since the second moment of Λ is $P/2$. This is the same effective SNR encountered in the proof of Theorem 5 and the rest of the proof follows identically from (79) onwards. ■

Proof of Theorem 3: See Figures 7 and 8 for block diagrams of the encoding and decoding processes. Choose $\epsilon > 0$. Encoder ℓ maps its finite field message vectors $\mathbf{w}_\ell^R$ and $\mathbf{w}_\ell^I$ to a lattice points $\mathbf{t}_\ell^R, \mathbf{t}_\ell^I \in \Lambda_\ell \cap \mathcal{V}$, using ϕ from Lemma 5,

$$\mathbf{t}_\ell^R = \phi(\mathbf{w}_\ell^R), \qquad \mathbf{t}_\ell^I = \phi(\mathbf{w}_\ell^I)\ . \quad (108)$$

Using Theorem 5, these lattice points can be transmitted across the channel so that the relays can make estimates $\hat{\mathbf{v}}_m^R$ and $\hat{\mathbf{v}}_m^I$ of lattice equations $\mathbf{v}_m^R$ and $\mathbf{v}_m^I$ with coefficient vectors $\mathbf{a}_m \in \{\mathbb{Z} + j\mathbb{Z}\}^L$ such that $\Pr\big(\cup_m\big\{\{\hat{\mathbf{v}}_m^R \neq \mathbf{v}_m^R\} \cup \{\hat{\mathbf{v}}_m^I \neq \mathbf{v}_m^I\}\big\}\big) < \epsilon$ for n large enough so long as

$$R_\ell < \min_{m:a_{m\ell}\neq 0} \log^+\left(\frac{P}{|\alpha_m|^2 + P\|\alpha_m \mathbf{h}_m - \mathbf{a}_m\|^2}\right)$$

for some $\alpha_1, \ldots, \alpha_M \in \mathbb{R}$. Finally, using ϕ^{-1} from Lemma 6, each relay can produce estimates of the desired linear combinations of messages, $\hat{\mathbf{u}}_m^R = \phi^{-1}(\hat{\mathbf{v}}_m^R)$ and $\hat{\mathbf{u}}_m^I = \phi^{-1}(\hat{\mathbf{v}}_m^I)$, such $\Pr\big(\cup_m\big\{\{\hat{\mathbf{u}}_m^R \neq \mathbf{u}_m^R\} \cup \{\hat{\mathbf{u}}_m^I \neq \mathbf{u}_m^I\}\big\}\big) < \epsilon$ where

$$\mathbf{u}_m^R = \bigoplus_{\ell=1}^{L}\Big(q_{m\ell}^R \mathbf{w}_\ell^R \oplus (-q_{m\ell}^I)\mathbf{w}_\ell^I\Big) \quad (109)$$

$$\mathbf{u}_m^I = \bigoplus_{\ell=1}^{L}\Big(q_{m\ell}^I \mathbf{w}_\ell^R \oplus q_{m\ell}^R \mathbf{w}_\ell^I\Big) \quad (110)$$

$$q_{m\ell}^R = g^{-1}\Big(\big[\mathsf{Re}(a_{m\ell})\big] \bmod p\Big) \quad (111)$$

$$q_{m\ell}^I = g^{-1}\Big(\big[\mathsf{Im}(a_{m\ell})\big] \bmod p\Big)\ . \quad (112)$$

C. Multi-Stage Networks

The framework developed in this section can easily be applied to AWGN networks with more than one layer of relays. Once the first layer has recovered its equations, it can just treat them as a set of messages for the second layer. The second layer simply decodes equations with coefficients that are close to the channel coefficients. This process repeats until the equations reach a destination. Since these layered equations are all linear, they can be expressed as linear equations over the original messages.

VI. Recovering Messages

The primary goal of compute-and-forward is to enable higher achievable rates across an AWGN network. Relays decode linear equations of transmitted messages and pass them towards the destination nodes which, upon receiving enough equations, attempt to solve for their desired messages. In this

$$[\mathbf{s}_m^R] \bmod \Lambda = \left[\sum_{\ell=1}^{L}\left(\mathsf{Re}(\alpha_m h_{m\ell})\mathsf{Re}(\mathbf{x}_\ell) - \mathsf{Im}(\alpha_m h_{m\ell})\mathsf{Im}(\mathbf{x}_\ell) + \mathsf{Re}(a_{m\ell})\mathbf{d}_\ell^R - \mathsf{Im}(a_{m\ell})\mathbf{d}_\ell^I\right) + \mathsf{Re}(\alpha_m \mathbf{z}_m)\right] \bmod \Lambda \quad (98)$$

$$= \left[\sum_{\ell=1}^{L}\left(\mathsf{Re}(a_{m\ell})(\mathsf{Re}(\mathbf{x}_\ell) + \mathbf{d}_\ell^R) - \mathsf{Im}(a_{m\ell})(\mathsf{Im}(\mathbf{x}_\ell) + \mathbf{d}_\ell^I) + \theta_{m\ell}^R\mathsf{Re}(\mathbf{x}_\ell) - \theta_{m\ell}^I\mathsf{Im}(\mathbf{x}_\ell)\right) + \mathsf{Re}(\alpha_m \mathbf{z}_m)\right] \bmod \Lambda \quad (99)$$

$$\overset{(a)}{=} \left[\sum_{\ell=1}^{L}\left(\mathsf{Re}(a_{m\ell})\mathbf{t}_\ell^R - \mathsf{Im}(a_{m\ell})\mathbf{t}_\ell^I + \theta_{m\ell}^R\mathsf{Re}(\mathbf{x}_\ell) - \theta_{m\ell}^I\mathsf{Im}(\mathbf{x}_\ell)\right) + \mathsf{Re}(\alpha_m \mathbf{z}_m)\right] \bmod \Lambda \quad (100)$$

$$\overset{(b)}{=} \left[\mathbf{v}_m^R + \sum_{\ell=1}^{L}\left(\theta_{m\ell}^R\mathsf{Re}(\mathbf{x}_\ell) - \theta_{m\ell}^I\mathsf{Im}(\mathbf{x}_\ell)\right) + \mathsf{Re}(\alpha_m \mathbf{z}_m)\right] \bmod \Lambda \quad (101)$$

section, we give sufficient conditions for recovering messages from a given set of equations.

It will be useful to represent the equations in matrix form. For real-valued channels let $\mathbf{Q} = \{q_{m\ell}\}$ be the matrix of equation coefficients. For complex-valued channels, let $\mathbf{Q}^R = \{q_{m\ell}^R\}$ and $\mathbf{Q}^I = \{q_{m\ell}^I\}$ be the real and imaginary coefficient matrices. Using this representation, we can write out the received equations for real-valued channels in matrix form,

$$\begin{bmatrix}\mathbf{u}_1 & \cdots & \mathbf{u}_M\end{bmatrix}^T = \mathbf{Q}\begin{bmatrix}\mathbf{w}_1 & \cdots & \mathbf{w}_L\end{bmatrix}^T .$$

Similarly, for complex-valued channels, we can write

$$\begin{bmatrix}\mathbf{u}_1^R & \cdots & \mathbf{u}_M^R & \mathbf{u}_1^I & \cdots & \mathbf{u}_M^I\end{bmatrix}^T = \begin{bmatrix}\mathbf{Q}^R & -\mathbf{Q}^I \\ \mathbf{Q}^I & \mathbf{Q}^R\end{bmatrix}\begin{bmatrix}\mathbf{w}_1^R & \cdots & \mathbf{w}_L^R & \mathbf{w}_1^I & \cdots & \mathbf{w}_L^I\end{bmatrix}^T .$$

These matrix formulations immediately yield sufficient conditions for recovery.

Theorem 7: For real-valued channels, a destination, given M linear combinations of messages with coefficient matrix $\mathbf{Q} \in \mathbb{F}_p^{M\times L}$, can recover all messages if and only if $\mathbf{Q}$ has rank L.

Theorem 8: For complex-valued channels, a destination, given M linear combinations of messages with real and imaginary coefficient matrices $\mathbf{Q}^R, \mathbf{Q}^I \in \mathbb{F}_p^{M\times L}$, can recover all messages if and only if both $\mathbf{Q}^R$ and $\mathbf{Q}^I$ have rank L.

In many cases, a destination may only be interested in a subset of the transmitted messages. Depending on the coefficients, it may be able to reduce the number of required equations. Recall that δ_ℓ is the unit vector with 1 in the ℓ^{th} entry and 0 elsewhere.

Theorem 9: For real-valued channels, a destination, given M linear combinations of messages with coefficient matrix $\mathbf{Q} \in \mathbb{F}_p^{M\times L}$, can recover the message $\mathbf{w}_\ell$ if there exists a vector $\mathbf{c} \in \mathbb{F}_p^M$ such that $\mathbf{c}^T\mathbf{Q} = \delta_\ell^T$.

Theorem 10: For complex-valued channels, a destination, given M linear combinations of messages with real and imaginary coefficient matrices $\mathbf{Q}^R, \mathbf{Q}^I \in \mathbb{F}_p^{M\times L}$, can recover the message $\mathbf{w}_\ell$ if there exists a vector $\mathbf{c} \in \mathbb{F}_p^{2M}$ such that

$$\mathbf{c}^T\begin{bmatrix}\mathbf{Q}^R & -\mathbf{Q}^I \\ \mathbf{Q}^I & \mathbf{Q}^R\end{bmatrix} = \delta_\ell^T . \quad (113)$$

Proof: Clearly, the vector $\mathbf{c}$ can be applied to the received equations $[\mathbf{u}_1^R \ \cdots \ \mathbf{u}_M^R \ \mathbf{u}_1^I \ \cdots \ \mathbf{u}_M^I]^T$ to recover $\mathbf{w}_\ell^R$. Let $\mathbf{c}^R$ denote the first M elements of $\mathbf{c}$, $\mathbf{c}^I$ denote the last M elements, and let $\tilde{\mathbf{c}} = [-\mathbf{c}^I \ \mathbf{c}^R]$. By symmetry, replacing $\mathbf{c}$ with $\tilde{\mathbf{c}}$ in (113) will yield the unit vector $\delta_{\ell+L}^T$ instead of δ_ℓ^T. Thus, $\tilde{\mathbf{c}}$ can be used to extract $\mathbf{w}_\ell^I$ from the equations. ■

Remark 9: These conditions can also be stated directly in terms of the coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_M$. For real-valued channels, set $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_M]^T$. Now, we can substitute $\mathbf{Q}$ with $\mathbf{A}$ in Theorems 7 and 9 so long as all operations are taken modulo p. For complex-valued channels, the same holds true for Theorems 8 and 10 if we replace $\mathbf{Q}^R$ with $\mathsf{Re}(\mathbf{A})$ and $\mathbf{Q}^I$ with $\mathsf{Im}(\mathbf{A})$.

It may be more convenient to evaluate the rank of the coefficients directly on the complex field. This is possible, given some mild assumptions on the equation coefficients.

Theorem 11: Assume that, in an AWGN network, the magnitude of each equation coefficient is upper bounded by a constant a_{MAX}. Then, for sufficiently large blocklength n and field size p, there exists a set of nested lattice codes such that a destination can recover all L messages from L equations if their coefficient matrix $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_L]^T$ is full rank over the complex field.

Proof: $\mathbf{A}$ is full rank over the complex field if and only if its real-valued representation $\tilde{\mathbf{A}}$ is full rank over the reals. Recall that a matrix is full rank only if its determinant is non-zero. We will now show that for sufficiently large p, if the determinant of $\tilde{\mathbf{A}}$ is non-zero over the reals it is non-zero modulo p. The determinant over $\mathbb{R}$ can be written as

$$\det(\tilde{\mathbf{A}}) = \sum_{\sigma\in\mathcal{S}} \text{sgn}(\sigma) \prod_{m=1}^{2L} \tilde{a}_{m\sigma(m)} \quad (114)$$

where $\mathcal{S}$ is the set of all permutations of $\{1, 2, \ldots, 2L\}$, $\text{sgn}(\sigma)$ is the signature of the permutation which is equal to 1 for even permutations and -1 for odd permutations, and $\tilde{a}_{m\ell}$ are the entries of $\tilde{\mathbf{A}}$. Using the upper bound on the magnitudes of the $a_{m\ell}$ and the fact that $|\mathcal{S}| = (2L)!$, the determinant is lower and upper bounded as follows:

$$-(2L)!(a_{\text{MAX}})^{2L} \le \det(\tilde{\mathbf{A}}) \le (2L)!(a_{\text{MAX}})^{2L} . \quad (115)$$

The determinant under modulo p arithmetic can be written as

$$\left[\sum_{\sigma\in\mathcal{S}} \text{sgn}(\sigma) \prod_{m=1}^{2L} \tilde{a}_{m\sigma(m)}\right] \bmod p \ . \tag{116}$$

Since the underlying field size $p \to \infty$ as $n \to \infty$, for large enough blocklength n, we can use the bounds on $\det(\tilde{\mathbf{A}})$ to show that the determinant modulo p does not wrap around zero. This immediately implies that it is zero if and only the determinant is zero over the reals. ■

Remark 10: Theorem 11 can also be stated in terms of bounds on the channel coefficients. For instance, if $|h_{m\ell}| < h_{\text{MAX}}$, then we can use the bound in Lemma 1, to show that $|a_{m\ell}|$ is bounded as well. More generally, the result holds if the channel coefficients are drawn from a distribution such that $Pr\left(\cup_{m\ell}\{|h_{m\ell}| > h_{\text{MAX}}\}\right) \to 0$ as $h_{\text{MAX}} \to \infty$. In this case, we choose h_{MAX} such that this probability is very small and can be absorbed into the total probability of error for our scheme. The result follows by taking an appropriate increasing sequence of h_{MAX}.

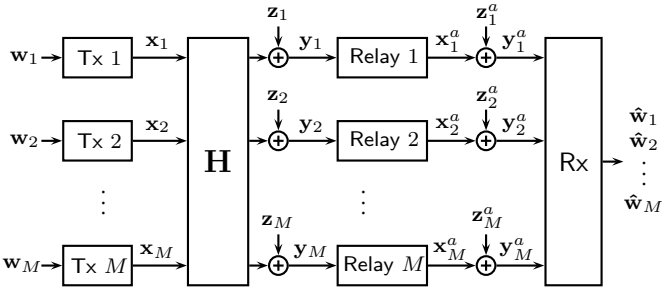

Fig. 9. A linear relay network where compute-and-forward is beneficial.

Example 4: Consider the AWGN network in Figure 9. Transmitters 1 through M send messages $\mathbf{w}_1, \ldots, \mathbf{w}_M$ through a channel $\mathbf{H}$ to M relays. Each relay has a point-to-point AWGN channel to the receiver which wants to recover all of the messages at the highest possible symmetric rate. Each channel input has power P and all noise terms are i.i.d. circularly symmetric Gaussian with variance 1. Let $\mathbf{H}$ be an $M \times M$ Hadamard matrix. (We assume that M is chosen such that a Hadamard matrix of that size exists.) Recall that a Hadamard matrix has ± 1 entires such that $\mathbf{H}\mathbf{H}^T = M\mathbf{I}$.

Using Theorems 4 and 11 and setting the coefficient vectors equal to the channel vectors, $\mathbf{a}_m = \mathbf{h}_m$, compute-and-forward can achieve

$$R_{\text{COMP}} = \log^+\left(\frac{1}{M} + P\right) \tag{117}$$

bits per channel use per user since $\mathbf{H}$ is full rank. It can be shown that decode-and-forward, amplify-and-forward, and compress-and-forward (with i.i.d. Gaussian codebooks) can achieve

$$R_{\text{DF}} = \frac{1}{M}\log\left(1 + MP\right) \tag{118}$$

$$R_{\text{AF}} = R_{\text{CF}} = \log\left(1 + P\left(\frac{P}{MP+1}\right)\right) \tag{119}$$

bits per channel use per user. Compute-and-forward is the dominant strategy except at very low power and it rapidly approaches the upper bound $R_{\text{UPPER}} = \log(1+P)$ as $P \to \infty$. As M increases the rates of decode-and-forward, amplify-and-forward, and compress-and-forward go to 0.

VII. Successive Cancellation

Once a relay has recovered an equation of messages, it can subtract its contribution from the channel observation. This results in a residual channel output from which it can extract a different equation, potentially with a higher rate than possible over the original channel. One key difference from standard applications of successive cancellation is that the relay cannot completely cancel out all channel inputs associated with the decoded equation. This is because in the first step, it only decodes an integer combination of the messages, which is often not the same as the linear combination taken by the channel.

We demonstrate an achievable region for decoding two different equations using successive cancellation at each relay. This can be easily generalized to more than two equations. For succinctness, we only state this result for real-valued channel models.

Theorem 12: Let $\mathbf{h}_1, \ldots, \mathbf{h}_M \in \mathbb{R}^L$ denote the channel vectors and R_ℓ denote the message rates. Each relay can first decode an equation with coefficient vector $\mathbf{a}_m \in \mathbb{Z}^L$ and then one with coefficient vectors $\mathbf{b}_m \in \mathbb{Z}^L$ if

$$R_\ell < \min\left(\min_{m:a_{m\ell}\neq 0} \mathcal{R}_1(\mathbf{h}_m, \mathbf{a}_m), \min_{m:b_{m\ell}\neq 0} \mathcal{R}_2(\mathbf{h}_m, \mathbf{a}_m, \mathbf{b}_m)\right)$$

$$\mathcal{R}_1(\mathbf{h}_m, \mathbf{a}_m) = \frac{1}{2}\log^+\left(\frac{P}{\alpha_m^2 + P\|\alpha_m\mathbf{h}_m - \mathbf{a}_m\|^2}\right)$$

$$\mathcal{R}_2(\mathbf{h}_m, \mathbf{a}_m, \mathbf{b}_m) = \begin{cases} \frac{1}{2}\log^+\left(\frac{P}{\beta_m^2 + P\sum_{\ell\neq i}|\beta_m h_{m\ell} - b_{m\ell}|^2}\right), & \mathbf{a}_m = \delta_i, \\ \frac{1}{2}\log^+\left(\frac{P}{\beta_m^2 + P\|\beta_m\mathbf{h}_m - \tau_m\mathbf{a}_m - \mathbf{b}_m\|^2}\right), & \text{otherwise.} \end{cases}$$

for some choice of $\alpha_m, \beta_m \in \mathbb{R}$ and $\tau_m \in \mathbb{Z}$.

Proof: All messages are mapped onto lattice points, dithered, and transmitted across the channel as in the proof of Theorem 3. The first set of equations can be reliably decoded using the procedure from Theorem 3 as well. Now, we condition on the event that each relay has successfully recovered the equation with coefficient vectors $\mathbf{a}_m$.

Consider the case where the first coefficient vector at relay m is a unit vector $\mathbf{a}_m = \delta_i$. This means that relay m can successfully decode the message $\mathbf{w}_i$ from encoder i. It can then replicate the encoding process to get $\mathbf{x}_i$. Now, the relay removes $\mathbf{x}_i$ from $\mathbf{y}_m$,

$$\mathbf{y}_m - h_{mi}\mathbf{x}_i = \sum_{\ell\neq i} h_{m\ell}\mathbf{x}_\ell + \mathbf{z}_m \ , \tag{120}$$

and uses this as a channel output for Theorem 1 to get the equation with coefficient vector $\tilde{\mathbf{b}}_m$ which is equal to $\mathbf{b}_m$ except that it has 0 in the i^{th} position. It then adds $b_{mi}\mathbf{w}_i$ to the recovered equation to get $\mathbf{b}_m$.

If $\mathbf{a}_m$ is not a unit vector, the decoder has access to the lattice equation

$$\mathbf{v}_m = \left[\sum_{\ell=1}^{L} a_{m\ell}\mathbf{t}_\ell\right] \bmod \Lambda \tag{121}$$

from which it computes

$$\begin{aligned}\bar{\mathbf{v}}_m &= \left[\mathbf{v}_m - \sum_{\ell=1}^{L} a_{m\ell}\mathbf{d}_\ell\right] \bmod \Lambda = \left[\sum_{\ell=1}^{L} a_{m\ell}\mathbf{x}_\ell\right] \bmod \Lambda \\ \tilde{\mathbf{y}}_m &= \left[\beta_m\mathbf{y}_m - \tau_m\bar{\mathbf{v}}_m\right] \bmod \Lambda \\ &= \left[\sum_{\ell=1}^{L}(\beta_m h_{m\ell} - \tau_m a_{m\ell})\mathbf{x}_\ell + \mathbf{z}_m\right] \bmod \Lambda\ .\end{aligned}$$

Now we can follow the steps in the proof of Theorem 5. In (67), replace $\alpha_m\mathbf{y}_m$ with $\tilde{\mathbf{y}}_m$. In all steps of the proof, substitute $a_{m\ell}$ with $b_{m\ell}$, $\alpha_m h_{m\ell}$ with $\beta_m h_{m\ell} - \tau_m a_{m\ell}$, and, if it has not already been replaced, α_m with β_m. ■

Remark 11: Given $\mathbf{a}_m$, $\mathbf{b}_m$, and τ_m, we can solve for the optimal α_m and β_m following the steps of the proof of Theorem 2.

Remark 12: The restriction of τ_m to the integers stems from the fact that (36) only holds for integer coefficients.

Example 5: There are $L = 4$ transmitters and $M = 1$ relay and the channel vector is $\mathbf{h}_1 = [10\ 10\ 8\ 8]^T$. The relay wants to first decode the equation with coefficient vector $\mathbf{a}_1 = [1\ 1\ 1\ 1]^T$ and then with coefficient vector $\mathbf{b}_1 = [1\ \ 1\ -1\ -1]^T$. Using Theorem 12, this is possible if the message rates satisfy

$$R_\ell < \min\left(\frac{1}{2}\log^+\left(\frac{1}{4} + \frac{81P}{1+4P}\right), \frac{1}{2}\log^+\left(\frac{1}{328} + P\right)\right)$$

by using $\tau_1 = 9$ so that $\mathbf{h}_1 - \tau_1\mathbf{a}_1 = \mathbf{b}_1$. Note that if we applied Theorem 1 directly to decode $\mathbf{b}_1$, we would not be able to get a positive rate.

Remark 13: As noted in Remark 7, it may be more efficient to recover an equation piecewise by recovering equations of subsets of messages and taking an appropriate linear combination of these equations. Theorem 12 is strictly better for this process than Theorem 1.

A. Multiple-Access

Assume there is only one relay and that it wants to recover all transmitted messages. This is the standard Gaussian multiple-access problem whose capacity region is well-known to be the set of all rate tuples $(R_1, \ldots, R_L)$ satisfying

$$\sum_{\ell\in S} R_\ell \ < \ \frac{1}{2}\log\left(1 + P\sum_{\ell\in S}|h_{1\ell}|^2\right) \tag{122}$$

for all subsets $S \subseteq \{1, 2, \ldots, L\}$ [72, Theorem 14.3.5]. We now show that compute-and-forward includes the multiple-access capacity region as a special case. First, we consider the corner point of the capacity region associated with decoding the messages in ascending order. From Example 2, the first message can be decoded (while treating the others as noise) if

$$R_1 < \frac{1}{2}\log\left(1 + \frac{|h_{11}|^2 P}{1 + P\sum_{i=2}^{L}|h_{1i}|^2}\right). \tag{123}$$

Using successive cancellation, the relay removes $\mathbf{x}_1$ from the channel observation to get $\sum_{\ell=2}^{L} h_{1\ell}\mathbf{x}_\ell + \mathbf{z}_1$. It then repeats the above procedure for each message in ascending order to get

$$R_\ell < \frac{1}{2}\log\left(1 + \frac{|h_{1\ell}|^2 P}{1 + P\sum_{i=\ell+1}^{L}|h_{1i}|^2}\right). \tag{124}$$

The resulting rate tuple is a corner point of the multiple-access capacity region. By changing the decoding order, any corner point is achievable. Note that any point on the boundary of the capacity region is achievable by time-sharing corner points.

Remark 14: One interesting open problem is to develop *joint decoding* for the compute-and-forward framework. Of course, within the context of multiple-access, this is possible with nested lattice codewords as they have good statistical properties. Extending joint decoding to recovering equations of messages may enlarge the computation rate region.

VIII. Superposition

In the previous section, we considered the scenario where each relay decodes several equations, but the transmitters each use a single codebook (as in Theorem 1). However, when decoding multiple equations, it is sometimes useful to superimpose multiple codebooks. We investigate this possibility in this section for real-valued channels. As before, the complex case follows naturally.

We will assume that there are two levels A and B and that each relay wants to a recover an equation from both levels. (If it is not interested in a level, it can just set its desired coefficients to zero.)

Each encoder has two messages $\mathbf{w}_{\ell A}$ and $\mathbf{w}_{\ell B}$ with rates $R_{\ell A}$ and $R_{\ell B}$ respectively. Relay m wants to decode equations $\mathbf{u}_{mA}$ and $\mathbf{u}_{mB}$ with coefficient vectors $\mathbf{a}_m$ and $\mathbf{b}_m$, respectively, for $m = 1, 2, \ldots, M$. In the theorem below, we give achievable rates for this scenario by combining superposition and successive cancellation. The basic idea is to superimpose two lattice codes at each receiver scaled by $\gamma_{\ell A}$ and $\gamma_{\ell B}$ to ensure that the power constraint is met.

Theorem 13: Choose $\gamma_{\ell A}, \gamma_{\ell B}$ such that $\gamma_{\ell A}^2 + \gamma_{\ell B}^2 = 1$. For channel vectors $\mathbf{h}_1, \ldots, \mathbf{h}_M \in \mathbb{R}^L$, the relays can first decode any set of linear equations over $\mathbf{w}_{\ell A}$ with coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_M \in \mathbb{Z}^L$ and then any set of linear equations over $\mathbf{w}_{\ell B}$ with coefficient vectors $\mathbf{b}_1, \ldots, \mathbf{b}_M \in \mathbb{Z}^L$ if

$$\begin{aligned}R_{\ell A} &< \min_{m:a_{m\ell}\neq 0} \frac{1}{2}\log^+\left(\frac{P}{N_{mA}}\right) \\ R_{\ell B} &< \min_{m:b_{m\ell}\neq 0} \frac{1}{2}\log^+\left(\frac{P}{N_{mB}}\right)\end{aligned}$$

where

$$\mathbf{h}_{mA} = [\gamma_{1A} h_{m1} \ \cdots \ \gamma_{LA} h_{mL}]^T$$
$$\mathbf{h}_{mB} = [\gamma_{1B} h_{m1} \ \cdots \ \gamma_{LB} h_{mL}]^T$$
$$N_{mA} = |\alpha_m|^2(1 + P\|\mathbf{h}_{mB}\|^2) + P\|\alpha_m \mathbf{h}_{mA} - \mathbf{a}_m\|^2$$
$$N_{mB1} = |\beta_m|^2(1 + P\sum_{\ell \neq i} |\gamma_{\ell A} h_{m\ell}|^2) + P\|\beta_m \mathbf{h}_{mB} - \mathbf{b}_m\|^2$$
$$N_{mB2} = |\beta_m|^2 + P\|\beta_m \mathbf{h}_{mA} - \tau_m \mathbf{a}_m\|^2 + P\|\beta_m \mathbf{h}_{mB} - \mathbf{b}_m\|^2$$
$$N_{mB} = \begin{cases} N_{mB1}, & \mathbf{a}_m = \delta_i \text{ for some } i, \\ N_{mB2}, & \text{otherwise.} \end{cases}$$

for some choice of $\alpha_m, \beta_m \in \mathbb{R}$ and $\tau_m \in \mathbb{Z}$.

Proof: Choose two sets of nested lattices $\Lambda \subset \Lambda_{LA} \subset \cdots \subset \Lambda_{1A}$, $\Lambda \subset \Lambda_{LB} \subset \cdots \subset \Lambda_{1B}$ with appropriate rates where Λ is the coarse lattice with second moment P. Each encoder maps its messages onto lattice points using ϕ from Lemma 5 and dithers them with $\mathbf{d}_{\ell A}, \mathbf{d}_{\ell B}$ drawn independently and uniformly over the fundamental Voronoi region $\mathcal{V}$ of Λ,

$$\mathbf{t}_{\ell A} = \phi_A(\mathbf{w}_{\ell A}) \qquad \mathbf{t}_{\ell B} = \phi_B(\mathbf{w}_{\ell B})$$
$$\mathbf{x}_{\ell A} = [\mathbf{t}_{\ell A} - \mathbf{d}_{\ell A}] \bmod \Lambda \qquad \mathbf{x}_{\ell B} = [\mathbf{t}_{\ell B} - \mathbf{d}_{\ell B}] \bmod \Lambda$$

It then combines $\mathbf{x}_{\ell A}$ and $\mathbf{x}_{\ell B}$ according to $\gamma_{\ell A}$ and $\gamma_{\ell B}$ which guarantees the power constraint is met:

$$\mathbf{x}_\ell = \gamma_{\ell A} \mathbf{x}_{\ell A} + \gamma_{\ell B} \mathbf{x}_{\ell B} \tag{125}$$
$$E[\|\mathbf{x}_\ell\|^2] = \gamma_{\ell A}^2 nP + \gamma_{\ell B}^2 nP = nP \tag{126}$$

At each receiver, we can just treat the channel output as if it came from $2L$ transmitters labelled $1A, \ldots, LA, 1B, \ldots, LB$. We can write the channel to receiver m and the desired coefficient vectors as

$$\tilde{\mathbf{h}}_m = \begin{bmatrix} \mathbf{h}_{mA} \\ \mathbf{h}_{mB} \end{bmatrix} \qquad \tilde{\mathbf{a}}_m = \begin{bmatrix} \mathbf{a}_m \\ \mathbf{0} \end{bmatrix} \qquad \tilde{\mathbf{b}}_m = \begin{bmatrix} \mathbf{0} \\ \mathbf{b}_m \end{bmatrix}.$$

We can now directly apply Theorem 12 with $\tilde{\mathbf{h}}_m$, $\tilde{\mathbf{a}}_m$, and $\tilde{\mathbf{b}}_m$ to get the desired result. ∎

Remark 15: As before, given $\mathbf{a}_m$, $\mathbf{b}_m$, τ_m, and $\gamma_{\ell A}$ we can solve for the optimal α_m and β_m following the steps of the proof of Theorem 2.

Remark 16: In order to keep the notation manageable, we have chosen to present the superposition strategy in Theorem 13 only for two levels. There are several immediate extensions, including:

- More than two levels.
- Allowing a different decoding order at each relay.
- Equations spanning different levels.

Example 6: There are $L = 3$ transmitters and $M = 1$ relay and the channel vector is $\mathbf{h}_1 = [1 \ 1 \ \sqrt{2}]^T$. Set the scaling coefficients to be $\gamma_{1A} = \gamma_{2A} = 0$, $\gamma_{1B} = \gamma_{2B} = 1$, and $\gamma_{3A} = \gamma_{3B} = 1/\sqrt{2}$. The relay wants to first decode the equation with coefficient vector $\mathbf{a}_1 = [0 \ 0 \ 1]^T$ from level A and then the equation with coefficient vector $\mathbf{b}_1 = [1 \ 1 \ 1]^T$ from level B. Using Theorem 13, this is possible if the message rates satisfy

$$R_{3A} < \frac{1}{2} \log\left(1 + \frac{P}{1+3P}\right) \tag{127}$$
$$R_{\ell B} < \frac{1}{2} \log^+\left(\frac{1}{3} + P\right) \qquad \ell = 1, 2, 3. \tag{128}$$

Remark 17: It can be shown that nested lattice codes can approach the capacity region of the standard Gaussian broadcast problem. See [16] for more details.

Remark 18: For an application of this superposition scheme to a backhaul-limited cellular uplink network, see [48].

IX. Outage Formulation

So far, we have considered fixed channel coefficients. Now, we demonstrate that our scheme can be applied to the slow fading scenario. This further emphasizes the fact that our compute-and-forward scheme does *not* require channel state information at the transmitters. Under a slow fading model, the channel matrix $\mathbf{H}$ is chosen according to some probability distribution and then remains fixed for all time. As a result, we must accept some probability that the rate used by the transmitters is above the maximum rate permitted for those channel coefficients. For an achievable strategy with rate $R_{\text{SCHEME}}(\mathbf{H})$ for fixed $\mathbf{H}$, this *outage probability* is given by

$$\rho_{\text{OUT}}(R) = \Pr\left(R_{\text{SCHEME}}(\mathbf{H}) < R\right) \ . \tag{129}$$

We can also characterize the performance of a given strategy by its *outage rate*,

$$R_{\text{OUT}}(\rho) = \sup\{R : \rho_{\text{OUT}}(R) \leq \rho\}. \tag{130}$$

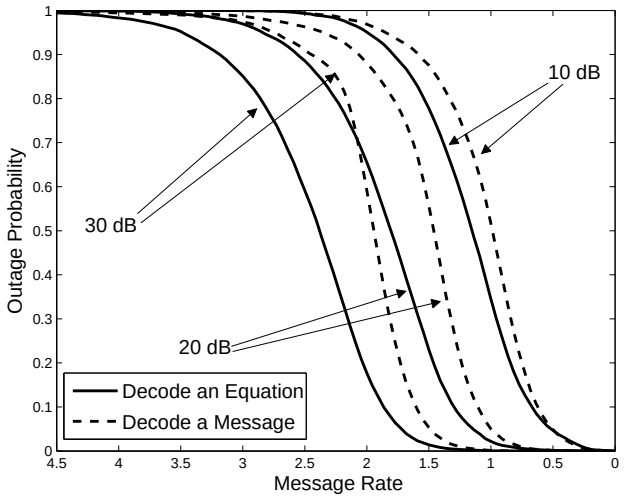

Fig. 10. Outage probability for a relay that receives $\mathbf{y} = h_1\mathbf{x}_1 + h_2\mathbf{x}_2 + h_3\mathbf{x}_3 + \mathbf{z}$ where the h_ℓ are i.i.d. according to $\mathcal{N}(0,1)$. The "Decode a Message" strategy uses standard random codes and joint typicality decoding to recover at least one of the messages $\mathbf{w}_1, \mathbf{w}_2$, or $\mathbf{w}_3$. The "Decode an Equation" strategy uses compute-and-forward to recover some linear equation $a_1\mathbf{w}_1 \oplus a_2\mathbf{w}_2 \oplus a_3\mathbf{w}_3$.

Example 7: There are three transmitters that communicate to a single relay over a real-valued AWGN multiple-access

channel. The channel coefficients h_ℓ are i.i.d. according to $\mathcal{N}(0,1)$ and are only known to the relay. Each transmitter has a single message $\mathbf{w}_\ell$ of rate R. Usually, the relay would only have the choice of decoding one message, two messages, or all three messages with the rates given by the multiple-access rate region.[5] The resulting outage probabilities for this strategy are plotted in Figure 10 for $P = 10, 20,$ and 30dB. We also plot the performance of the compute-and-forward strategy from Theorem 1, which permits the relay to decode any linear equation of the messages, $\mathbf{u} = \bigoplus_\ell a_\ell \mathbf{w}_\ell$ so long as at least one of the coefficients is not equal to zero.

The example above demonstrates that decoding an equation is often easier than decoding a message. In order to use compute-and-forward for network communication, we also need that the end-to-end linear transformation of the desired messages is full rank. The next section explores this issue through a case study.

X. Case Study: Distributed MIMO

We will now compare the outage performance of compute-and-forward to the performance of classical relaying strategies over a simple network. Consider the two user distributed MIMO network in Figure 11. There are two sources, two relays, and one destination. The relays see the transmitters through $\mathbf{H}$ whose entries are i.i.d. Rayleigh, $h_{m\ell} \sim \mathcal{CN}(0,1)$. We assume that relay m only knows the channel vector $\mathbf{h}_m$ to itself. Each relay is given a bit pipe with rate R_0 bits per channel use to the destination. The destination would like to recover both message $\mathbf{w}_1$ and $\mathbf{w}_2$ at the highest possible symmetric outage rate. Recall that for a symmetric rate point to be achievable, both transmitters must be able to communicate their messages with at least that rate.

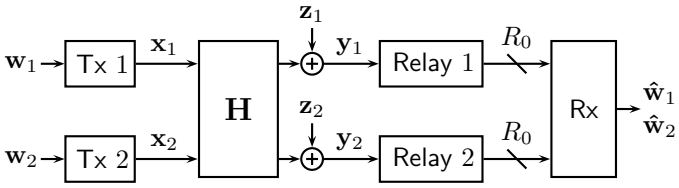

Fig. 11. Two transmitters communicate to a distributed MIMO receiver with two antennas. Each antenna has a rate R_0 bit pipe to the receiver.

The basic compute-and-forward strategy has each relay decode the equation with the highest rate and pass that to the destination. If the equations received by the destination are full rank, decoding is successful. However, at low SNR, the probability that the equations are not full rank is quite high as shown in Figure 13. One simple solution is to force each relay to choose an equation with $a_{mm} \neq 0$. This results in equations that are far more likely to be solvable at the expense of slightly lower computation rates.[6] The achievable rates for these two strategies are given below and are plotted in Figure 12 for $R_0 = 2$ and outage probability $\rho = 1/4$.

[5]Those messages that are not decoded are treated as noise.

[6]More work is needed to develop distributed coefficient selection strategies that operate on the optimal tradeoff between computation rate and matrix rank.

$$R_{\text{MAX},m} = \max_{\mathbf{a}_m} \log^+ \left(\left(\|\mathbf{a}_m\|^2 - \frac{P\,|\mathbf{h}_m^* \mathbf{a}_m|^2}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right)$$

$$R_{\text{NZ},m} = \max_{\substack{\mathbf{a}_m \\ a_{mm}\neq 0}} \log^+ \left(\left(\|\mathbf{a}_m\|^2 - \frac{P\,|\mathbf{h}_m^* \mathbf{a}_m|^2}{1+P\|\mathbf{h}_m\|^2} \right)^{-1} \right)$$

$$R_{\text{COMP}}(\mathbf{H}) = \begin{cases} \min\left(\left(\min_m R_{\text{MAX},m} \right), R_0 \right) & \mathsf{rank}(\mathbf{A}) = 2, \\ 0 & \text{otherwise.} \end{cases}$$

$$R_{\text{CNZ}}(\mathbf{H}) = \begin{cases} \min\left(\left(\min_m R_{\text{NZ},m} \right), R_0 \right) & \mathsf{rank}(\mathbf{A}) = 2, \\ 0 & \text{otherwise.} \end{cases}$$

For decode-and-forward, we require that each relay is responsible for a single message. It attempts to recover this message either by treating the other message as noise or decoding both messages. The rate for this strategy is evaluated below and plotted in Figure 12. For more details on decode-and-forward for multiple relays (as well as compress-and-forward and cut-set upper bounds), see [3].

$$R_{\text{ignore},1} = \log\left(1 + \frac{|h_{11}|^2 P}{1+|h_{12}|^2 P}\right) \tag{131}$$

$$R_{\text{ignore},2} = \log\left(1 + \frac{|h_{22}|^2 P}{1+|h_{21}|^2 P}\right) \tag{132}$$

$$R_{\text{decode},m} = \min\Bigg(\log\left(1+|h_{m1}|^2 P\right), \log\left(1+|h_{m2}|^2 P\right), \frac{1}{2}\log\left(1+\|\mathbf{h}_m\|^2 P\right) \Bigg) \tag{133}$$

$$R_{\text{ii}} = \min(R_{\text{ignore},1}, R_{\text{ignore},2}) \tag{134}$$

$$R_{\text{id}} = \min(R_{\text{ignore},1}, R_{\text{decode},2}) \tag{135}$$

$$R_{\text{di}} = \min(R_{\text{decode},1}, R_{\text{ignore},2}) \tag{136}$$

$$R_{\text{dd}} = \min(R_{\text{decode},1}, R_{\text{decode},2}) \tag{137}$$

$$R_{\text{DF}}(\mathbf{H}) = \min\left(\max(R_{\text{ii}}, R_{\text{id}}, R_{\text{di}}, R_{\text{dd}}), R_0 \right) \tag{138}$$

For our upper bound, we use a cut-set bound that either groups the relays with the sources or with the destination. This yields the following bound on the symmetric rate:

$$R_{\text{MIMO}}(\mathbf{H}) = \min\Bigg(\log\left(1+(|h_{11}|^2+|h_{21}|^2)P\right), \log\left(1+(|h_{12}|^2+|h_{22}|^2)P\right), \frac{1}{2}\log\det\left(\mathbf{I}+\mathbf{H}\mathbf{H}^* P\right) \Bigg) \tag{139}$$

$$R_{\text{UPPER}}(\mathbf{H}) = \min\left(R_{\text{MIMO}}(\mathbf{H}), R_0\right) . \tag{140}$$

Finally, we consider the performance of compress-and-forward with i.i.d. Gaussian codebooks. The variance of the channel observation at relay m is $1 + \|\mathbf{h}_m\|^2 P$ and we have to compress this using R_0 bits. At the destination, one can equivalently write this as a MIMO channel with channel matrix

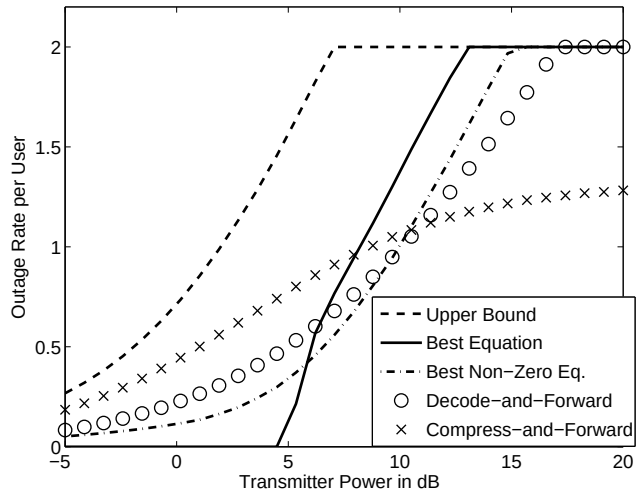

Fig. 12. Symmetric outage rates for the 2-user distributed MIMO multiple-access channel with i.i.d. Rayleigh fading only known at the receivers. Here, we set $R_0 = 2$ and outage probability $\rho = 1/4$.

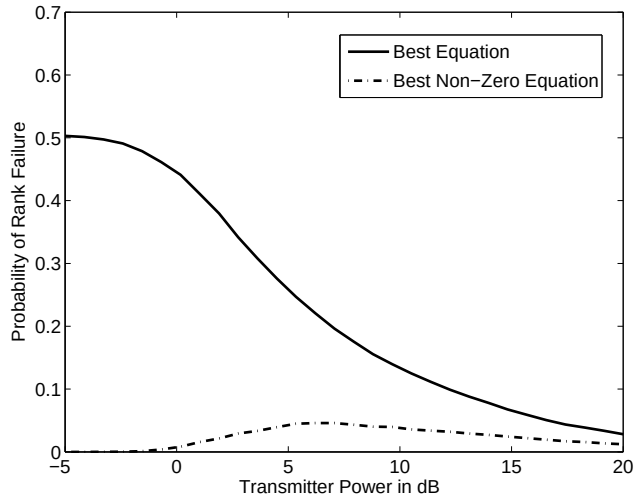

Fig. 13. Probability of rank failure for the 2-user distributed MIMO multiple-access channel by having each relay decode the best equation and the best non-zero equation.

$\mathbf{H}_{\text{CF}}$,

$$\mathsf{SNR}_{\text{CF},m} = \frac{P(2^{R_0}-1)}{2^{R_0}+P\|\mathbf{h}_m\|^2} \tag{141}$$

$$\mathbf{H}_{\text{CF}} = \begin{bmatrix} \sqrt{\mathsf{SNR}_{\text{CF},1}/P} & 0 \\ 0 & \sqrt{\mathsf{SNR}_{\text{CF},2}/P} \end{bmatrix} \mathbf{H} \tag{142}$$

$$R_{\text{CF}}(\mathbf{H}) = R_{\text{MIMO}}(\mathbf{H}_{\text{CF}}) \ . \tag{143}$$

From Figure 12, we can see that compute-and-forward (with the best equation) outperforms all other strategies starting at approximately 8dB. It also saturates the bit pipes to the destination using 5dB less power per transmitter than required for decode-and-forward. However, the gains are not as dramatic as observed in Example 4. For non-integer coefficients, we can only decode an integer combination and the remainder acts like additional noise. Despite this penalty, compute-and-forward is the best strategy in the moderate transmit power regime. Compress-and-forward is a good strategy at low transmit power since, in this regime, the rate of the bit pipes exceeds the MIMO capacity between the transmitters and the relays. Therefore, the effective noise introduced by vector quantization at the relays does not significantly degrade the effective end-to-end SNR. At high transmit power, this effective noise becomes a significant factor. Decode-and-forward is not as efficient as compute-and-forward at high transmit power as the relays must either treat one of the messages as noise or decode both. However, it outperforms compute-and-forward in the low transmit power regime since it is able to perform joint decoding.[7]

Remark 19: Note that the encoding strategy for compute-and-forward does not depend on the choice of equation coefficients at the relay. Therefore, one can obtain the maximum of the best equation rate and the best non-zero equation rate with the same strategy simply by disallowing certain coefficients at the relays past an appropriate P.

Remark 20: Since the channel from the transmitters to the relays is essentially a 2-user interference channel, it may be useful to have each transmitter send out a public and a private message as in the Han-Kobayashi scheme [62]. Such a scheme might improve the performance of both the decode-and-forward strategy and the compute-and-forward strategy (by employing superposition as in Section VIII).

XI. Upper Bound

In this section, we give a simple upper bound on the computation rate through a genie-aided argument. This bound does not match our achievable strategy in general and it may be possible to construct tighter outer bounds by taking into account the mismatch between the desired function and the function naturally provided by the channel.

Theorem 14: Assume the channel between the transmitters and the relays is $p(y_1,\ldots,y_M|x_1,\ldots,x_L)$. If the relays, want equations with coefficient vectors $\mathbf{a}_1,\ldots,\mathbf{a}_M \in \mathbb{Z}^L$, the message rates are upper bounded as follows:

$$R_\ell \le \min_{m:a_{m\ell}\neq 0} I(X_\ell; Y_m|X_1,\ldots,X_{\ell-1},X_{\ell+1},\ldots,X_L)$$

For the real-valued Gaussian channel model considered in this paper, with channel vectors $\mathbf{h}_1,\ldots,\mathbf{h}_M \in \mathbb{R}^L$, this specializes to

$$R_\ell \le \min_{m:a_{m\ell}\neq 0} \frac{1}{2}\log\left(1+h_{m\ell}^2 P\right) \ . \tag{144}$$

Similarly, for the complex-valued Gaussian channel model considered in this paper, with coefficient vectors $\mathbf{a}_1,\ldots,\mathbf{a}_M \in \{\mathbb{Z}+j\mathbb{Z}\}^L$ channel vectors $\mathbf{h}_1,\ldots\mathbf{h}_M \in \mathbb{C}^L$, we have that

$$R_\ell \le \min_{m:a_{m\ell}\neq 0} \log\left(1+|h_{m\ell}|^2 P\right) \ . \tag{145}$$

Proof: To each relay m for which $a_{m\ell} \neq 0$, we provide all messages except that from encoder ℓ as genie-aided side-information. Now, we are left with a multicasting problem

[7]We do not know how to naturally fit joint decoding into the compute-and-forward framework so we have excluded it (even in the context of multiple-access) to emphasize this fact.

from encoder ℓ to all relays with $a_{m\ell} \neq 0$. Clearly, the multicast rate is upper bounded by the lowest rate link. For the Gaussian case, it is easy to show that the mutual information expressions are maximized by the Gaussian distribution. ■

XII. Conclusions

In this paper, we have developed a new coding scheme that enables relays to reliably recover equations of the original messages by exploiting the interference structure of the wireless channel. As we have seen, this framework can achieve end-to-end rates across an AWGN network that are not accessible with classical relaying strategies. More generally, the techniques in this paper can be used as building blocks for developing new cooperative communication schemes that exploit both the algebraic and statistical properties of wireless networks. Here, we presented an application to distributed MIMO and we believe there are many other scenarios where it will be useful. For instance, it can reduce energy consumption for gossiping over a sensor network [73] and improve the performance of low-complexity MIMO receiver architectures [74].

Compute-and-forward also adds to the growing pile of evidence that structured codes are a powerful tool for tackling problems in multi-user information theory. Recently, many new inner bounds have emerged that take advantage of the algebraic structure of multi-user problems. The behavior observed in these strategies is not well-captured by the usual cut-set outer bounds. Therefore, new outer bounds that account for algebraic as well as statistical structure will be needed to better characterize the capacity regions of multi-user networks [75]. An interesting direction for future study, inspired by the work of Avestimehr, Diggavi, and Tse on deterministic models [76], is whether compute-and-forward can be used to closely approximate the capacity of an AWGN network.

Acknowledgment

The authors would like to thank G. Reeves for pointing out Theorem 2 when this work was in an early stage. They would also like to thank G. Bresler, U. Erez, S. Shamai, and R. Zamir for valuable discussions as well as the anonymous reviewers whose comments improved the presentation of this work.

Appendix A
Upper Bound on Noise Densities

In this appendix, we demonstrate that the densities of the noise terms in Theorem 5 and 6 are upper bounded by the density of an i.i.d. Gaussian vector. The proof follows that of Lemmas 6 and 11 from [15].

Lemma 8: Let $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}^{n\times n})$ and let $\mathbf{d}_\ell$ be independently generated according to a uniform distribution over $\mathcal{V}$, the fundamental Voronoi region of Λ. Also, let $\sigma^2_{\mathcal{B}}$ denote the second moment of an n-dimensional ball whose radius is equal to the covering radius r_{COV} of Λ and let $\mathbf{z}^*_\ell$ be independently generated according to $\mathcal{N}(\mathbf{0}, \sigma^2_{\mathcal{B}}\mathbf{I}^{n\times n})$. Now, let

$$\mathbf{z}_{eq} = \alpha\mathbf{z} + \sum_{\ell=1}^{L} \theta_\ell \mathbf{d}_\ell \tag{146}$$

where $\alpha, \theta_\ell \in \mathbb{R}$. There exists an i.i.d. Gaussian vector

$$\mathbf{z}^* = \alpha\mathbf{z} + \sum_{\ell=1}^{L} \theta_\ell \mathbf{z}^*_\ell \tag{147}$$

with variance σ^2 satisfying

$$\sigma^2 \leq \alpha^2 + \left(\frac{r_{\text{COV}}}{r_{\text{EFFEC}}}\right)^2 P \sum_{\ell=1}^{L} \theta_\ell^2 \tag{148}$$

such that the density of $\mathbf{z}_{eq}$ is upper bounded as follows:

$$f_{\mathbf{z}_{eq}}(\mathbf{z}) \leq e^{Lc(n)n} f_{\mathbf{z}^*}(\mathbf{z}) \tag{149}$$

$$c(n) = \ln\left(\frac{r_{\text{COV}}}{r_{\text{EFFEC}}}\right) + \frac{1}{2}\ln 2\pi e G^{(n)}_{\mathcal{B}} + \frac{1}{n} \tag{150}$$

where $\ln$ is the natural logarithm, $G^{(n)}_{\mathcal{B}}$ is the normalized second moment of an n-dimensional ball, and r_{EFFEC} is the effective radius of Λ.

Proof: First, we will show that the density of $\mathbf{z}_{eq}$ is upper bounded as desired. From Lemma 11 in [15], we have that

$$f_{\mathbf{d}_\ell}(\mathbf{z}) \leq e^{c(n)n} f_{\mathbf{z}^*_\ell}(\mathbf{z}) \ . \tag{151}$$

Since $\mathbf{z}, \mathbf{d}_1, \ldots, \mathbf{d}_L$ are independent, we can write the density of $\mathbf{z}_{eq}$ as an n-dimensional convolution of the densities of its components,

$$f_{\mathbf{z}_{eq}}(\mathbf{z}) = f_{\alpha\mathbf{z}}(\mathbf{z}) * f_{\theta_1\mathbf{d}_1}(\mathbf{z}) * \cdots * f_{\theta_L\mathbf{d}_L}(\mathbf{z}) \ . \tag{152}$$

Similarly, we can write the density of $\mathbf{z}^*$ as

$$f_{\mathbf{z}^*}(\mathbf{z}) = f_{\alpha\mathbf{z}}(\mathbf{z}) * f_{\theta_1\mathbf{z}^*_1}(\mathbf{z}) * \cdots * f_{\theta_L\mathbf{z}^*_L}(\mathbf{z}) \ . \tag{153}$$

Since probability densities are non-negative, we can use the upper bound in (151) to get

$$f_{\alpha\mathbf{z}}(\mathbf{z}) * f_{\theta_\ell\mathbf{d}_\ell}(\mathbf{z}) \leq f_{\alpha\mathbf{z}}(\mathbf{z}) * e^{c(n)n} f_{\theta_\ell\mathbf{z}^*_\ell}(\mathbf{z}) \ . \tag{154}$$

Applying this idea L times to $f_{\mathbf{z}_{eq}}(\mathbf{z})$ yields

$$f_{\mathbf{z}_{eq}}(\mathbf{z}) \leq e^{Lc(n)n} f_{\mathbf{z}^*}(\mathbf{z}) \ . \tag{155}$$

We must now upper bound the variance of $\mathbf{z}^*$. By Definition 19, $\mathsf{Vol}(\mathcal{B}(r_{\text{EFFEC}})) = \mathsf{Vol}(\mathcal{V})$. Recall that a ball has the smallest second moment for a given volume. Let $\mathbf{b}$ be generated according to the uniform distribution over $\mathcal{B}(r_{\text{COV}})$. It follows that

$$P = \frac{1}{n}E\left[\|\mathbf{d}_\ell\|^2\right] \tag{156}$$

$$\geq \frac{1}{n}E\left[\left\|\frac{r_{\text{EFFEC}}}{r_{\text{COV}}}\mathbf{b}\right\|^2\right] = \left(\frac{r_{\text{EFFEC}}}{r_{\text{COV}}}\right)^2 \sigma^2_{\mathcal{B}} \ . \tag{157}$$

Finally, we get

$$\sigma^2 = \frac{1}{n}E\left[\|\alpha\mathbf{z}\|^2\right] + \frac{1}{n}\sum_{\ell=1}^{L} E\left[\|\theta_\ell\mathbf{z}^*_\ell\|^2\right] \tag{158}$$

$$= \alpha^2 + \sigma^2_{\mathcal{B}}\sum_{\ell=1}^{L}\theta_\ell^2 \tag{159}$$

$$\leq \alpha^2 + \left(\frac{r_{\text{COV}}}{r_{\text{EFFEC}}}\right)^2 P\sum_{\ell=1}^{L}\theta_\ell^2 \ . \tag{160}$$

■

Since the coarse lattice is good for covering and for quantization, $\frac{r_{\text{COV}}}{r_{\text{EFFEC}}} \to 1$ and $G_{\mathcal{B}}^{(n)} \to \frac{1}{2\pi e}$ as $n \to \infty$. Therefore, $c(n) \to 0$ as $n \to \infty$. As we will show in the next appendix, the fine lattices are good for AWGN, which means that they can attain a positive error exponent for i.i.d. Gaussian noise whose variance is smaller than their respective second moments.

APPENDIX B
FINE LATTICES ARE GOOD FOR AWGN

We now show that the fine lattices from Section IV-B can recover from i.i.d. Gaussian noise.

Lemma 9: $\Lambda_1, \Lambda_2, \ldots, \Lambda_L$ are good for AWGN with probability that goes to 1 as $n \to \infty$ so long as $\frac{n}{p} \to 0$.

Proof: Recall that the coarse lattice Λ is good for AWGN. Let $\tilde{\mathcal{C}}_\ell$ be a codebook consisting of length n codewords randomly and independently generated according to a uniform distribution over $\mathcal{V}$, the fundamental Voronoi region of Λ. Let $\tilde{\mathbf{z}}_\ell$ denote an i.i.d. Gaussian vector with zero-mean and any variance σ_ℓ^2 such that the volume-to-noise ratio $\mu(\Lambda_\ell, \epsilon) = \frac{(\mathsf{Vol}(\mathcal{V}))^{2/n}}{\sigma_\ell^2}$ is greater than $2\pi e$. Consider the following channel from $\tilde{\mathbf{x}}_\ell \in \tilde{\mathcal{C}}_\ell$ to $\tilde{\mathbf{y}}_\ell \in \mathcal{V}$:

$$\tilde{\mathbf{y}}_\ell = [\tilde{\mathbf{x}}_\ell + \tilde{\mathbf{z}}_\ell] \mod \Lambda \tag{161}$$

and let ϵ_ℓ the probability that $\tilde{\mathbf{x}}_\ell$ is incorrectly decoded from $\tilde{\mathbf{y}}_\ell$. As part of the proof of Theorem 5 in [15], it is shown that the random coding error exponent for this channel is equal to the Poltyrev exponent (see Equation (56) in [15]). This means that ϵ_ℓ decreases exponentially with n for volume-to-noise ratio greater than $2\pi e$. Appendix C of [15] shows that the same performance is possible via Euclidean decoding if $\tilde{\mathbf{x}}_\ell$ is drawn according to a uniform distribution over $\{p^{-1}\Lambda\} \cap \mathcal{V}$ and $\frac{n}{p} \to 0$.

From Lemma 3, we know that the marginal distribution of each element of $\Lambda_\ell \cap \mathcal{V}$ is uniform over $\{p^{-1}\Lambda\} \cap \mathcal{V}$. Furthermore, all points in the set $\Lambda_\ell \cap \mathcal{V}$ are pairwise independent. This is all that is required to apply the union bound and obtain the same performance as i.i.d. inputs over $\{p^{-1}\Lambda\} \cap \mathcal{V}$ in terms of the error exponent.

Thus, the probability that Λ_ℓ is good for AWGN (with the Poltyrev error exponent) goes to 1 as $n \to \infty$. It follows from the union bound that $\Lambda_1, \ldots, \Lambda_L$ are simultaneously good for AWGN with high probability as $n \to \infty$. ∎

APPENDIX C
FIXED DITHERS

We now show that there exist fixed dithers that are appropriate for our coding scheme. Instead of setting the second moment of Λ to P, we will set the covering radius r_{COV} to $\sqrt{nP}$. Recall that the covering radius is chosen such that the resulting ball $\mathcal{B}(r_{\text{COV}})$ includes every point of the fundamental Voronoi region $\mathcal{V}$. Therefore, setting $r_{\text{COV}} = \sqrt{nP}$ guarantees that every transmission $\mathbf{x}_\ell \in \mathcal{V}$ satisfies the power constraint. We now show that the rate loss can be made arbitrarily small.

The effective radius r_{EFFEC} is chosen such that $\mathsf{Vol}(\mathcal{V}) = \mathsf{Vol}(\mathcal{B}(r_{\text{EFFEC}}))$. Recall that, for even n, the volume of an n-dimensional ball of radius 1 is

$$\mathsf{Vol}(\mathcal{B}(1)) = \frac{\pi^{n/2}}{(n/2)!} . \tag{162}$$

By Stirling's approximation, for any $\delta > 0$ and n large enough, this is lower bounded by

$$\mathsf{Vol}(\mathcal{B}(1)) \geq \left(\frac{2\pi e}{n(1+\delta)}\right)^{n/2} . \tag{163}$$

Thus, for any δ and n large enough, the volume of Vol satisfies

$$\begin{aligned}
\mathsf{Vol}(\mathcal{V}) = \mathsf{Vol}(\mathcal{B}(r_{\text{EFFEC}})) &= \left(\frac{r_{\text{EFFEC}}}{r_{\text{COV}}}\right)^n \mathsf{Vol}(\mathcal{B}(r_{\text{COV}})) \\
&\geq \left(\frac{r_{\text{EFFEC}}}{r_{\text{COV}}}\right)^n \left(\frac{2\pi e\ r_{\text{COV}}^2}{n(1+\delta)}\right)^{n/2} \\
&= \left(\frac{r_{\text{EFFEC}}}{r_{\text{COV}}}\right)^n \left(\frac{2\pi e\ P}{(1+\delta)}\right)^{n/2} .
\end{aligned}$$

Since Λ is also good for covering, we can choose n large enough such that $r_{\text{COV}}^2 / r_{\text{EFFEC}}^2 > 1/(1+\delta)$. Finally, we have that

$$\mathsf{Vol}(\mathcal{V}) \geq \left(\frac{2\pi e\ P}{(1+\delta)^2}\right)^{n/2} . \tag{164}$$

Substituting this bound into (84), we can see that this only reduces the rate by an additional $\log(1+\delta)$ bits, which can be made arbitrarily small through our choice of δ.

Note that the probability of error decays exponentially in n averaged over the randomness in the dither vectors and the noise. Therefore, for n large enough, there is at least one good fixed set of dither vectors that attains the desired probability of error ϵ.

REFERENCES

[1] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, pp. 572–584, September 1979.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, pp. 3062–3080, December 2004.

[3] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Transactions on Information Theory*, vol. 51, pp. 3037–3063, September 2005.

[4] A. El Gamal, N. Hassanpour, and J. Mammen, "Relay networks with delays," *IEEE Transactions on Information Theory*, vol. 53, pp. 3413–3431, October 2007.

[5] Y.-H. Kim, "Capacity of a class of deterministic relay channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 1328–1329, March 2008.

[6] M. Aleksic, P. Razaghi, and W. Yu, "Capacity of a class of modulo-sum relay channels," *IEEE Transactions on Information Theory*, vol. 55, pp. 921–930, March 2009.

[7] A. Sanderovich, O. Somekh, H. V. Poor, and S. Shamai (Shitz), "Uplink macro diversity of limited backhaul cellular network," *IEEE Transactions on Information Theory*, vol. 55, pp. 3457–3478, August 2009.

[8] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Noisy network coding," *IEEE Transactions on Information Theory*, vol. 57, pp. 3132–3152, May 2011.

[9] 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.

[10] M. Gastpar and M. Vetterli, "On the capacity of large Gaussian relay networks," *IEEE Transactions on Information Theory*, vol. 51, pp. 765–779, March 2005.

[11] 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, pp. 3302–3318, October 2007.

[12] 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.

[13] V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Communications Magazine*, vol. 12, pp. 3–11, February 2005.

[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 and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, pp. 2293–2314, October 2004.

[16] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, pp. 1250–1276, June 2002.

[17] H. E. Gamal, G. Caire, and M. O. Damen, "Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of MIMO channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 968–985, June 2004.

[18] R. Ahlswede, "Group codes do not achieve Shannon's channel capacity for general discrete channels," *The Annals of Mathematical Statistics*, vol. 42, pp. 224–240, February 1971.

[19] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *European Transactions on Telecommunications*, vol. 19, pp. 455–474, June 2008.

[20] 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.

[21] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Transactions on Information Theory*, vol. 53, pp. 3498–3516, October 2007.

[22] T. Philosof and R. Zamir, "On the loss of single-letter characterization: The dirty multiple access channel," *IEEE Transactions on Information Theory*, vol. 55, pp. 2442–2454, June 2009.

[23] T. Philosof, R. Zamir, U. Erez, and A. Khisti, "Lattice strategies for the dirty multiple access channel," *IEEE Transactions on Information Theory*, Submitted April 2009. See http://arxiv.org/abs/0904.1892.

[24] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, pp. 1204–1216, July 2000.

[25] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, pp. 371–381, February 2003.

[26] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 782–795, October 2003.

[27] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, pp. 4413–4430, October 2006.

[28] S. Zhang, S.-C. Liew, and P. Lam, "Hot topic: Physical-layer network coding," in *Proceedings of the 12th Annual ACM International Conference on Mobile Computing and Networking (MobiCom 2006)*, (Los Angeles, CA), September 2006.

[29] P. Popovski and H. Yomo, "Bi-directional amplification of throughput in a wireless multi-hop network," in *Proceedings of the 63rd IEEE Vehicular Technology Conference (VTC 2006 - Spring)*, (Melbourne, Australia), May 2006.

[30] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2006)*, (Seattle, WA), July 2006.

[31] B. Nazer and M. Gastpar, "Computing over multiple-access channels with connections to wireless network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2006)*, (Seattle, WA), July 2006.

[32] B. Nazer and M. Gastpar, "Lattice coding increases multicast rates for Gaussian multiple-access networks," in *45th Annual Allerton Conference on Communications, Control, and Computing*, (Monticello, IL), September 2007.

[33] K. Narayanan, M. P. Wilson, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," in *45th Annual Allerton Conference on Communications, Control, and Computing*, (Monticello, IL), September 2007.

[34] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Transactions on Information Theory*, vol. 11, pp. 5641–5654, November 2010.

[35] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity bounds for two-way relay channels," in *Proceedings of the International Zurich Seminar on Communications (IZS 2008)*, (Zurich, Switzerland), March 2008.

[36] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the gaussian two-way relay channel to within $1/2$ bit," *IEEE Transactions on Information Theory*, vol. 56, pp. 5488–5494, November 2010.

[37] W. Nam, S.-Y. Chung, and Y. H. Lee, "Nested lattice codes for Gaussian relay networks with interference," *IEEE Transactions on Information Theory*, Submitted February 2009. See http://arxiv.org/abs/0902.2436.

[38] S.-C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond," in *Physical Communication*, to appear 2011. See http://arxiv.org/abs/1105.4261.

[39] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the* IEEE, vol. 99, pp. 438–460, March 2011.

[40] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Transactions on Information Theory*, vol. 54, pp. 3457–3470, August 2008.

[41] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom for the K user interference channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425–3441, August 2008.

[42] G. Bresler, A. Parekh, and D. Tse, "The approximate capacity of the many-to-one and one-to-many gaussian interference channels," *IEEE Transactions on Information Theory*, vol. 56, pp. 4566–4592, September 2010.

[43] N. Khude, V. Prabhakaran, and P. Viswanath, "Harnessing bursty interference," in *Proceedings of the IEEE Information Theory Workshop (ITW 2009)*, (Volos, Greece), June 2009.

[44] S. Sridharan, A. Jafarian, S. Vishwanath, S. A. Jafar, and S. Shamai (Shitz), "A layered lattice coding scheme for a class of three user Gaussian interference channels," in *46th Annual Allerton Conference on Communications, Control, and Computing*, (Monticello, IL), September 2008.

[45] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath, "Ergodic interference alignment," in *Proceedings of the International Symposium on Information Theory (ISIT 2009)*, (Seoul, South Korea), June 2009.

[46] S.-W. Jeon and S.-Y. Chung, "Capacity of a class of multi-source relay networks," *IEEE Transactions on Information Theory*, Submitted July 2009. See http://arxiv.org/abs/0907.2510.

[47] A. Sanderovich, M. Peleg, and S. Shamai (Shitz), "Scaling laws in decentralized processing of interfered Gaussian channels," in *Proceedings of the International Zurich Seminar on Communications (IZS 2008)*, (Zurich, Switzerland), March 2008.

[48] B. Nazer, A. Sanderovich, M. Gastpar, and S. Shamai (Shitz), "Structured superposition for backhaul constrained cellular uplink," in *Proceedings of the International Symposium on Information Theory (ISIT 2009)*, (Seoul, South Korea), June 2009.

[49] D. Krithivasan and S. S. Pradhan, "Lattices for distributed source coding: Jointly Gaussian sources and reconstruction of a linear function," *IEEE Transactions on Information Theory*, vol. 55, pp. 5268–5651, December 2009.

[50] D. Krithivasan and S. Pradhan, "Distribued source coding using Abelian group codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 1495–1519, March 2011.

[51] A. B. Wagner, "On distributed compression of linear functions," *IEEE Transactions on Information Theory*, vol. 57, pp. 79–94, January 2011.

[52] A. D. Sarwate, B. Nazer, and M. Gastpar, "Spatial filtering in sensor networks with computation codes," in *Proceedings of the IEEE Statistical Signal Processing Workshop (SSP 2007)*, (Madison, WI), August 2007.

[53] B. Nazer and M. Gastpar, "Structured random codes and sensor network coding theorems," in *Proceedings of the International Zurich Seminar on Communications (IZS 2008)*, (Zurich, Switzerland), March 2008.

[54] R. Soundararajan and S. Vishwanath, "Communicating the difference of correlated Gaussian sources over a MAC," in *Data Compression Conference (DCC 2009)*, (Snowbird, UT), March 2009.

[55] Y. Kochman and R. Zamir, "Joint Wyner-Ziv/dirty-paper coding by modulo-lattice modulation," *IEEE Transactions on Information Theory*, vol. 55, pp. 4878–4889, November 2009.

[56] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," *IEEE Transactions on Information Theory*, Submitted July 2009. See http://arxiv.org/abs/0907.5388.
[57] S. Agrawal and S. Vishwanath, "On the secrecy rate of interference networks using structured codes," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2009)*, (Seoul, South Korea), June 2009.
[58] C. Feng, D. Silva, and F. Kschischang, "An algebraic approach to physical-layer network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2010)*, (Austin, TX), June 2010.
[59] B. Hern and K. Narayanan, "Multilevel coding schemes for compute-and-forward." See http://arxiv.org/abs/1010.1016.
[60] O. Ordentlich and U. Erez, "Achieving the gains promised by integer-forcing equalization with binary codes," in *Proceedings of the 26th IEEE Convention of Electrical and Electronics Engineerings in Israel (IEEEI 2010)*, (Eliat, Israel), November 2010.
[61] U. Erez and R. Zamir, "A modulo-lattice transformation for multiple-access channels," in *Proceedings of the 25th IEEE Convention of Electrical and Electronic Engineers in Israel*, (Eliat, Israel), December 2008.
[62] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Transactions on Information Theory*, vol. 27, pp. 49–60, January 1981.
[63] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Information Theory*, vol. 54, pp. 5534–5562, December 2008.
[64] U. Niesen and P. Whiting, "The degrees-of-freedom of compute-and-forward," *IEEE Transactions on Information Theory*, Submitted January 2011. See http://arxiv.org/abs/1101.2182.
[65] A. S. Motahari, S. O. Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Transactions on Information Theory*, Submitted November 2009. See http://arxiv.org/abs/0908.2282.
[66] C. A. Rogers, "Lattice coverings of space," *Mathematica*, vol. 6, pp. 33–39, 1959.
[67] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Transactions on Information Theory*, vol. 42, pp. 1152–1159, July 1996.
[68] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Transactions on Information Theory*, vol. 40, pp. 409–417, March 1994.
[69] 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.
[70] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Transactions on Information Theory*, vol. 43, pp. 1767–1773, November 1997.
[71] D. Krithivasan and S. Pradhan, "A proof of the existence of good lattices," tech. rep., University of Michigan, July 2007. See http://www.eecs.umich.edu/techreports/systems/cspl/cspl-384.pdf.
[72] T. Cover and J. Thomas, *Elements of Information Theory*. Hoboken, NJ: Wiley-Interscience, 2nd ed., 2006.
[73] B. Nazer, A. G. Dimakis, and M. Gastpar, "Local inteference can accelerate gossip algorithms," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, August 2011.
[74] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," in *IEEE Transactions on Information Theory*, To be submitted 2011.
[75] R. Etkin and E. Ordentlich, "The degrees-of-freedom of the k-user Gaussian interference channel is discontinuous at rational channel coefficients," *IEEE Transactions on Information Theory*, vol. 55, pp. 4932–4946, November 2009.
[76] S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, pp. 1872–1905, April 2011.

Bobak Nazer received the B.S.E.E. degree from Rice University, Houston, TX, in 2003, the M.S. degree from the University of California, Berkeley, CA, in 2005, and the Ph.D degree from the University of California, Berkeley, CA, in 2009, all in electrical engineering.

He is currently an Assistant Professor in the Department of Electrical and Computer Engineering at Boston University, Boston, MA. From 2009 to 2010, he was a postdoctoral associate in the Department of Electrical and Computer Engineering at the University of Wisconsin, Madison, WI. His research interests are in network information theory and statistical signal processing, with applications to wireless networks and distributed, reliable computation.

Dr. Nazer received the Eli Jury award from the EECS Department at UC - Berkeley in 2009 for his dissertation research and a Dean's Catalyst Award from Boston University in 2011. He is a member of Eta Kappa Nu, Tau Beta Pi, and Phi Beta Kappa.

Michael Gastpar received the Dipl. El.-Ing. degree from the Swiss Federal Institute of Technology (ETH), Zurich, in 1997, the M.S. degree from the University of Illinois at Urbana-Champaign, Urbana, in 1999, and the Doctorat ès Science degree from the Ecole Polytechnique Fédérale, Lausanne, Switzerland (EPFL), in 2002, all in electrical engineering. He was also a student in engineering and philosophy at the Universities of Edinburgh and Lausanne.

He is currently a Professor in the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale, Lausanne, Switzerland, and an Associate Professor in the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. He also holds a faculty position at Delft University of Technology and was a researcher at Bell Labs, Lucent Technologies, Murray Hill, NJ. His research interests are in network information theory and related coding and signal processing techniques, with applications to sensor networks and neuroscience.

Dr. Gastpar won the 2002 EPFL Best Thesis Award, an NSF CAREER award in 2004, and an Okawa Foundation Research Grant in 2008. He is an Information Theory Society Distinguished Lecturer (2009–2011). He is currently an Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY, and he has served as Technical Program Committee Co-Chair for the 2010 International Symposium on Information Theory, Austin, TX.