Approximately achieving Gaussian relay network capacity with lattice codes

Ayfer Özgür
EPFL, Lausanne, Switzerland
ayfer.ozgur@epfl.ch

Suhas Diggavi
UCLA, USA and EPFL, Switzerland
suhas@ee.ucla.edu

***Abstract*—Recently, it has been shown that a quantize-map-and-forward scheme approximately achieves (within a constant number of bits) the Gaussian relay network capacity for arbitrary topologies [1]. This was established using Gaussian codebooks for transmission and random mappings at the relays. In this paper, we show that the same approximation result can be established by using lattices for transmission and quantization along with structured mappings at the relays.**

I. Introduction

Characterizing the capacity of relay networks has been a long-standing open question in network information theory. The seminal work of Cover and El-Gamal [2] has established the basic achievability schemes for relay channels. More recently there has been extension of these techniques to larger networks (see [3] and references therein). In [1], motivated by a deterministic model of wireless communication, it was shown that the quantize-map-and-forward scheme achieves within a constant number of bits from the information-theoretic cutset upper bound. This constant is universal in the sense that it is independent of the channel gains and the operating SNR, though it could depend on the network topology (like the number of nodes).

In the quantize-map-and-forward scheme analyzed in [1], each relay node first quantizes its received signal at the noise level, then randomly maps it to a Gaussian codeword and transmits it. A natural question that we address in this paper is whether lattice codes retain the approximate optimality of the above scheme. This is motivated in part since lattice codes along with lattice decoding could enable computationally tractable encoding and decoding methods. For example lattice codes were used for linear function computation over multiple-access networks [4] and for communication over multiple-access relay networks (with orthogonal broadcast) in [5]. The main result of this paper is to show that the quantize-map-and-forward scheme using nested lattice codes for transmission and quantization, still achieves the Gaussian relay network capacity within a constant. This result is summarized in Theorem 2.1. The use of structured codes allows to specify a structured mapping between the quantization and transmission codebooks at each relay. The nested lattice codebooks considered in this paper are based on the random construction in [6], where they are shown to achieve the capacity of the AWGN channel.

This paper is organized as follows: In Section II, we state the network model and our main result. In Section III, we summarize the construction of the nested lattice ensemble. In Section IV, we describe the network operation. In particular, we specify how we use the nested lattice codes of Section III for encoding at the source, quantization, mapping and transmission at the relay nodes, and decoding at the destination node. In Section V, we analyse the performance achieved by the scheme. The detailed proofs can be found in [10].

II. Main Result

We consider a Gaussian relay network where a source node s wants to communicate to a destination node d, with the help of N relay nodes, denoted $\mathcal{N}$. The signal received by node $i \in \{s, d, \mathcal{N}\}$ is given by

$$\mathbf{y}_i = \sum_{j \neq i} H_{ij}\mathbf{x}_j + \mathbf{z}_i$$

where H_{ij} is the $N_i \times M_j$ channel matrix from node j comprising M_j transmit antennas to node i comprising N_i receive antennas. Each element of H_{ij} represents the complex channel gain from a transmitting antenna of node j to a receiving antenna of node i. The noise $\mathbf{z}_i$ is complex circularly-symmetric Gaussian vector $\mathcal{CN}(0, \sigma^2 I)$ and is i.i.d. for different nodes. The transmitted signals $\mathbf{x}_j$ are subject to an average power constraint P.

The following theorem is the main result of this paper.

Theorem 2.1: Using nested lattice codes for transmission and quantization along with structured mappings at the relays, we can achieve all rates

$$R \leq \min_{\Omega} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c}) - \sum_{i \in \mathcal{N}} N_i$$

between s and d, where Ω is a source-destination cut of the network and $X_\Omega = \{X_i,\, i \in \Omega\}$ are i.i.d. $\mathcal{CN}(0, (P/M_i)I)$.

It has been shown in [1] that the restriction to i.i.d. Gaussian input distributions is within $\sum_{i \in \mathcal{N},d} N_i$ bits/s/Hz of the cut-set upper bound. Therefore the rate achieved using lattice codes in the above theorem is within $2\sum_{i \in \mathcal{N},d} N_i$ bits/s/Hz to the cutset upper bound of the network.

For simplicity of presentation, in the rest of the paper we concentrate on a layered network where every node has a single transmit and receive antenna. More precisely, the signal received by node i in layer $l, 0 \leq l \leq l_d$, denoted $i \in \mathcal{N}_l$, is

given by

$$\mathbf{y}_i = \sum_{j \in \mathcal{N}_{l-1}} h_{ij}\mathbf{x}_j + \mathbf{z}_i$$

where h_{ij} is the real scalar channel coefficient from node j in layer $l-1$, to node i. $s \in \mathcal{N}_0$, $d \in \mathcal{N}_{l_d}$. The analysis can be extended to non-layered networks by following the time-expansion argument of [1], to multicast traffic with multiple destination nodes as well as to multiple multicast where multiple source nodes multicast to a group of destination nodes.

III. Construction of the Nested Lattice Ensemble

Consider a lattice Λ (or more precisely, a sequence of lattices $\Lambda^{(n)}$ indexed by the lattice dimension n) with $\mathcal{V}$ denoting the Voronoi region of Λ. Let us define the second moment per dimension of Λ as

$$\sigma^2(\Lambda) = \frac{1}{n}\frac{1}{V}\int_{\mathcal{V}} \|\mathbf{x}\|^2 d\mathbf{x}$$

where V denotes the volume of $\mathcal{V}$ and let the $n \times n$ full-rank generator matrix of Λ be denoted by G_Λ, i.e., $\Lambda = G_\Lambda \mathbb{Z}^n$. We assume that Λ (or more precisely, the sequence of lattices $\Lambda^{(n)}$) is both Roger's and Poltyrev good. The existence of such lattices has been shown in [7], where the reader can also find the precise definitions of Roger's and Poltyrev good. This fixed lattice Λ will serve as the coarse lattice for all our nested lattice constructions.

The fine lattice Λ_1 is constructed using Loeliger's type-A construction [8]. Let k, n, p be integers such that $k \leq n$ and p is prime. The fine lattice is constructed using the following steps.

- Draw an $n \times k$ matrix G such that each of its entries is i.i.d according to the uniform distribution over $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.
- Form the linear code
$$\mathcal{C} = \{\mathbf{c} : \mathbf{c} = G \cdot \mathbf{w}, \mathbf{w} \in \mathbb{Z}_p^k\}, \quad (1)$$
where "$\cdot$" denotes modulo-p multiplication.
- Lift $\mathcal{C}$ to $\mathbb{R}^n$ to form
$$\Lambda_1' = p^{-1}\mathcal{C} + \mathbb{Z}^n.$$
- $\Lambda_1 = G_\Lambda \Lambda_1'$ is the desired fine lattice. Note that since $\mathbb{Z}^n \subseteq \Lambda_1'$, we have $\Lambda \subseteq \Lambda_1$.
- Draw $\mathbf{v}$ uniformly over $p^{-1}\Lambda \cap \mathcal{V}$ and translate the lattice Λ_1 by $\mathbf{v}$. The nested lattice codebook consists of all points of the translated fine lattice inside the Voronoi region of the coarse lattice,
$$\Lambda^* = (\mathbf{v} + \Lambda_1) \mod \Lambda = (\mathbf{v} + \Lambda_1) \cap \mathcal{V}. \quad (2)$$

In the above equation, we define $\mathbf{x} \mod \Lambda$ as the quantization error of $\mathbf{x} \in \mathbb{R}^n$ with respect to the lattice Λ, i.e.,

$$\mathbf{x} \mod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}), \quad (3)$$

where the lattice quantizer $Q_\Lambda(\mathbf{x}) : \mathbb{R}^n \to \Lambda$ is given by

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

Note that the quantization and mod operations with respect to a lattice can be defined in different ways. The mod operation in (3) maps $\mathbf{x} \in \mathbb{R}^n$ to the Voronoi region $\mathcal{V}$ of the lattice. More generally, it is possible to define a mod or quantization operation with respect to any fundamental region of the lattice. In particular, when we consider the integer lattice $\mathbb{Z}^n$ in the sequel, or more generally its multiples $p\mathbb{Z}^n$ where p is a positive integer, we will assume that

$$\mathbf{x} \mod p\mathbb{Z}^n = \mathbf{x} - \lfloor \mathbf{x} \rfloor_p$$

where $\lfloor \mathbf{x} \rfloor_p$ denotes component-wise rounding to the nearest smaller integer multiple of p. In other words, the mod operation with respect to $p\mathbb{Z}^n$ maps the point $\mathbf{x} \in \mathbb{R}^n$ to the region $p\,[0,1)^n$.

The above construction yields a random ensemble of nested lattice codes that has the following desired properties:

- There is a bijection between
$$\mathbb{Z}_p^n \leftrightarrow p^{-1}\mathbb{Z}^n \cap [0,1)^n \leftrightarrow p^{-1}\Lambda \cap G_\Lambda\,[0,1)^n \leftrightarrow p^{-1}\Lambda \cap \mathcal{V}.$$

The last observation follows simply from the fact that both $G_\Lambda\,[0,1)^n$ and $\mathcal{V}$ are fundamental regions of the lattice Λ, i.e., they both tile $\mathbb{R}^n$. Since $\mathcal{C} \subseteq \mathbb{Z}_p^n$, the above bijection restricted to $\mathcal{C}$ yields,

$$\mathcal{C} \leftrightarrow p^{-1}\mathcal{C} = \Lambda_1' \cap [0,1)^n \leftrightarrow \Lambda_1 \cap G_\Lambda\,[0,1)^n \leftrightarrow \Lambda_1 \cap \mathcal{V} \leftrightarrow \Lambda^*. \quad (4)$$

Note that $\Lambda^* \subseteq p^{-1}\Lambda \cap \mathcal{V}$. The bijections above can be explicitly specified in both directions and we will make use of this fact in the next section.

The random codebook Λ^* has the following statistical properties:

- Let $\lambda \in p^{-1}\Lambda \cap \mathcal{V}$,
$$\mathbb{P}(\Lambda^*(i) = \lambda) = \frac{1}{|p^{-1}\Lambda \cap \mathcal{V}|} = \frac{1}{p^n}.$$
- Let $\lambda_1, \lambda_2 \in p^{-1}\Lambda \cap \mathcal{V}, \quad \forall i \neq j,$
$$\mathbb{P}(\Lambda^*(i) = \lambda_1, \Lambda^*(j) = \lambda_2) = \frac{1}{|p^{-1}\Lambda \cap \mathcal{V}|^2} = \frac{1}{p^{2n}}. \quad (5)$$

In other words, the construction in this section yields an ensemble of nested lattice codes such that each codeword of the random codebook Λ^* is uniformly distributed over $p^{-1}\Lambda \cap \mathcal{V}$ and the codewords of Λ^* are pairwise independent. These two properties suffice to prove the random coding result of this paper.

IV. Encoding, Mapping and Decoding

The above construction yields a random ensemble of nested lattice pairs $\Lambda \subseteq \Lambda_1$ with coding rate,

$$R = \frac{1}{n}\log|\Lambda^*|$$

which can be tuned by choosing the precise magnitudes of k and p. In this ensemble, the coarse lattice Λ is fixed and the fine lattice Λ_1 is randomized. It has been shown in [9] that with high probability, a nested lattice (Λ_1, Λ) in this ensemble is such that both Λ_1 and Λ are Roger's and Poltyrev-good. For quantization, we fix one such good member of the ensemble and use it at all the relay nodes. For transmission, we draw a random nested lattice codebook from this ensemble, independently at each relay. The mapping

between the quantization and transmission codebooks at each relay is specified below.

Source: The source has p^k messages, where p is prime and $k \leq n$. The messages are represented as length-k vectors over the finite field $\mathbb{Z}_p$ and mapped to a random nested lattice codebook Λ^* following the construction in Section III. In the construction, the coarse lattice Λ is scaled such that its second moment $\sigma^2(\Lambda^T) = (1-\epsilon_1(\Lambda))P$, where Λ^T now denotes the scaled version of the lattice Λ to satisfy the power constraint. $\epsilon_1(\Lambda) \to 0$ as n increases and choosing it carefully we can ensure that every codeword of Λ^* satisfies the power constraint P. The information transmission rate is given by

$$R = \frac{1}{n}\log p^k.$$

Let us denote by $\mathbf{x}_s^{(w)}$, $w \in \{1,\ldots,e^{nR}\}$ the random transmit codewords corresponding to each message w of the source node.

Relays: The relay node i receives the signal $\mathbf{y}_i$. The signal $\mathbf{y}_i$ is first quantized by using a nested lattice codebook that has been generated by the construction in Section III. It is shown in [9] that this construction yields nested lattices where the fine lattice is Roger's good with high probability if $k \geq (\log n)^2$. (The coarse lattice is both Roger's and Poltyrev good by construction.) We fix one such good nested lattice (Λ_1^Q, Λ^Q) and use the corresponding codebook $\Lambda_Q^* = \Lambda_1^Q \mod \Lambda^Q$ at all the relay nodes for quantization. Therefore our quantization codebook is not random but fixed and moreover same for all relay nodes. We assume that the nested lattice (Λ_1^Q, Λ^Q) has been generated by using the following parameters: Let

$$D_s = \max_i \sum_{j\in\mathcal{N}_{l-1}} |h_{ij}|^2 P. \tag{6}$$

The coarse lattice Λ^Q is a scaled version of the lattice Λ such that

$$\sigma^2(\Lambda^Q) = 2\mu(D_s + \sigma^2) \tag{7}$$

for a constant $\mu > 0$. Recall that σ^2 is the noise variance. We denote the generator matrix of the scaled coarse lattice Λ^Q by G_{Λ^Q} . The parameters k_r and p_r are chosen such that $k_r = (\log n)^2$ and p_r is the prime number such that[1]

$$p_r^k = e^{nR_r}, \qquad \text{where} \quad R_r = \frac{1}{2}\log\frac{\sigma^2(\Lambda^Q)}{\sigma^2}. \tag{8}$$

Note that since R_r is independent of n, $p_r = e^{\frac{nR_r}{(\log n)^2}}$, i.e, $p_r \to \infty$ as $n \to \infty$. It can be shown that with the choice in (8) for R_r, the second moment of Λ_1^Q is such that $\sigma^2(\Lambda_1^Q) \to \sigma^2$ when n increases. (This is a consequence of the fact that both Λ_1^Q and Λ^Q are Roger's good.) Therefore, we are effectively quantizing at the noise level.

The quantized signal is given by

$$\hat{\mathbf{y}}_i = Q_{\Lambda_1^Q}(\mathbf{y}_i + \mathbf{u}_i) \mod \Lambda^Q$$

where $\mathbf{u}_i$ is a random dither known at the destination node and uniformly distributed over the Voronoi region $\mathcal{V}_1^Q$ of the fine lattice Λ_1^Q. The dithers $\mathbf{u}_i$ are independent for different nodes.

Map and Forward: Let us scale the coarse lattice Λ such that its second moment $\sigma^2(\Lambda^T) = (1-\epsilon_1(\Lambda))P$. Let G_{Λ^T} denote the generator matrix of the scaled coarse lattice. The quantized signal $\hat{\mathbf{y}}_i$ at relay i is mapped to the transmitted signal $\mathbf{x}_i$ by the following mapping,

$$\mathbf{x}_i = G_{\Lambda^T}\, p_r^{-1}\, \left(G_i\, p_r\, \left(G_{\Lambda_Q}^{-1}\, \hat{\mathbf{y}}_i \mod \mathbb{Z}^n\right) \mod p_r\mathbb{Z}^n\right) + \mathbf{v}_i \mod \Lambda^T, \tag{9}$$

where G_i is an $n\times n$ random matrix with its entries uniformly and independently distributed in $0,1,\ldots,p_r-1$ and $\mathbf{v}_i$ is a random vector uniformly distributed over $p_r^{-1}\Lambda^T \cap \mathcal{V}^T$, where $\mathcal{V}^T$ is the Voronoi region of Λ^T. G_i and $\mathbf{v}_i$ are independent for different relay nodes. We index the e^{nR_r} codewords of Λ_Q^* as $\hat{\mathbf{y}}_i^{(k_i)}$, $k_i \in \{1,\ldots,e^{nR_r}\}$. The corresponding sequence that the codeword $\hat{\mathbf{y}}_i^{(k_i)}$ is mapped to in (9) is denoted by $\mathbf{x}_i^{(k_i)}$.

Proposition 4.1: The above mapping has the following properties:

- At each relay i, the transmitted sequences $\mathbf{x}_i \in \Lambda_i^*$, where Λ_i^* is a nested lattice codebook.
- The mapping induces a pairwise independent and uniform distribution over $p_r^{-1}\Lambda^T \cap \mathcal{V}^T$. Formally, each quantization codeword $\hat{\mathbf{y}}_i^{(k_i)} \in \Lambda_Q^*$ is mapped uniformly at random to the set $p_r^{-1}\Lambda^T \cap \mathcal{V}^T$. Two codewords $\hat{\mathbf{y}}_i^{(k_i)}, \hat{\mathbf{y}}_i^{(k_i')} \in \Lambda_Q^*$ such that $k_i \neq k_i'$ are mapped independently.
- The mapping induces an independent distribution across the relays.

The proposition says that the quantization codebooks at each relay are independently mapped to a random nested lattice codebook from the ensemble constructed in Section III. The proof is based on the bijection given in (4): There is one-to-one correspondence between the codebook Λ_Q^* and its underlying finite field codebook $\mathcal{C}^Q$. The mapping $p_r\,(G_{\Lambda^Q}^{-1}\,\hat{\mathbf{y}}_i \mod \mathbb{Z}^n)$ takes the codeword $\hat{\mathbf{y}}_i \in \Lambda_Q^*$ to its corresponding codeword in $\mathcal{C}^Q$. This codeword in $\mathcal{C}^Q$ is then mapped to a random finite-field codebook $\mathcal{C}_i = \left\{\mathbf{c}' : \mathbf{c}' = G_i\cdot\mathbf{c},\, \mathbf{c}\in\mathcal{C}^Q\right\}$. We then form the nested lattice codebook Λ_i^* corresponding to $\mathcal{C}_i$ following again the construction of Section III. The second property follows by observing that the random matrix G_i maps every nonzero vector $\mathbf{c}\in\mathcal{C}^Q$ uniformly at random to another finite field vector in $\mathbb{Z}_p^n$. The third property follows from the independence of the G_i's and $\mathbf{v}_i$'s for different nodes i.

The mapping in (9) can be simplified to the form,

$$\mathbf{x}_i = G_{\Lambda^T}\, G_i\, G_{\Lambda_Q}^{-1}\, \hat{\mathbf{y}}_i + \mathbf{v}_i \mod \Lambda^T.$$

Effectively, it takes the quantization codebook Λ_Q^*, expands it by multiplying with a random matrix with large entries (of the order of p_r) and then folds it to the Voronoi region of Λ^T. Since the entries of G_i are potentially very large, even if two codewords are close in Λ_Q^*, they are mapped independently to the codewords of the transmit codebook. Note that the complexity of the mapping is polynomial in n, while random mapping of the form in [1] has exponential complexity in n.

[1]More precisely, one should take p_r to be the largest prime number such that $p_r \leq e^{nR_r/k}$. When n is large, the difference becomes negligible.

Destination: Given its received signal $\mathbf{y}_d$, together with the knowledge of all codebooks, mappings, dithers and channel gains, the decoder performs a consistency check to recover the transmitted message. For each relay i and quantization codeword $\hat{\mathbf{y}}_i^{(k_i)}$, it first forms the signals

$$\tilde{\mathbf{y}}_i^{(k_i)} = \hat{\mathbf{y}}_i^{(k_i)} - \mathbf{u}_i \mod \Lambda^Q. \tag{10}$$

Note that for $i \in \mathcal{N}_l$

$$\begin{aligned}\tilde{\mathbf{y}}_i &= \hat{\mathbf{y}}_i - \mathbf{u}_i \mod \Lambda^Q \\ &= Q_{\Lambda_1^Q}(\mathbf{y}_i + \mathbf{u}_i) - \mathbf{u}_i \mod \Lambda^Q \\ &= (\mathbf{y}_i - (\mathbf{y}_i + \mathbf{u}_i) \mod \Lambda_1^Q) \mod \Lambda^Q \\ &= \sum_{j\in\mathcal{N}_{l-1}} h_{ij}\mathbf{x}_j + \mathbf{z}_i - \mathbf{u}_i' \mod \Lambda^Q, \end{aligned} \tag{11}$$

where $\mathbf{u}_i' = (\mathbf{y}_i + \mathbf{u}_i) \mod \Lambda_1^Q$. $\mathbf{u}_i'$ is independent of $\mathbf{y}_i$ and is uniform over the Voronoi region of Λ_1^Q (Crypto Lemma, see [6]).

The decoder then checks the set $\hat{\mathcal{W}}$ of messages $\hat{w}$ for which there exists some indices k_i, such that

$$(\mathbf{x}_s^{(\hat{w})}, \mathbf{y}_d, \{\tilde{\mathbf{y}}_i^{(k_i)}, \mathbf{x}_i^{(k_i)}\}_{i\in\mathcal{N}}) \in \widetilde{\mathcal{A}}_\epsilon$$

where $\widetilde{\mathcal{A}}_\epsilon$ denotes consistency and $\mathcal{N}$ denotes the set of relays. We define consistency as follows: For a given set of indices $\{k_i\}_{i\in\mathcal{N}}$, we say $(\mathbf{x}_s^{(\hat{w})}, \mathbf{y}_d, \{\tilde{\mathbf{y}}_i^{(k_i)}, \mathbf{x}_i^{(k_i)}\}_{i\in\mathcal{N}}) \in \widetilde{\mathcal{A}}_\epsilon$ if

$$\|(\tilde{\mathbf{y}}_i^{(k_i)} - \sum_{j\in\mathcal{N}_{l-1}} h_{ij}\mathbf{x}_j^{(k_j)}) \mod \Lambda^Q\|^2 \le n\,\sigma_c^2, \tag{12}$$

for all $i \in \mathcal{N}_l$, $1 \le l \le l_d$ where for convenience of notation we have denoted $\mathbf{x}_s^{(\hat{w})} = \mathbf{x}_j^{(k_j)}, j \in \mathcal{N}_0$, and $\mathbf{y}_d = \tilde{\mathbf{y}}_i^{(k_i)}, i \in \mathcal{N}_{l_d}$. We choose

$$\sigma_c^2 = (1+\epsilon)\,2\sigma^2$$

for a constant $\epsilon > 0$ that can be taken arbitrarily small. We can interpret the consistency check as follows. For each layer $l = 1, \ldots, l_d - 1$ the decoders picks a set of potential (quantized) received sequences $\{\hat{\mathbf{y}}_i^{(k_i)}\}_{i\in\mathcal{N}_l}$ and the transmit sequences corresponding to them $\{\mathbf{x}_i^{(k_i)}\}_{i\in\mathcal{N}_l}$. It checks for each layer l, whether the inputs and outputs are consistent, i.e., whether the examined inputs $\{\mathbf{x}_i^{(k_i)}\}_{i\in\mathcal{N}_{l-1}}$ of the layer l could have generated the examined outputs $\{\hat{\mathbf{y}}_i^{(k_i)}\}_{i\in\mathcal{N}_l}$. Note that the termination conditions are known, i.e., $\mathbf{x}_s$ is known for the message being tested, and $\mathbf{y}_d$ is the observed sequence at the destination. Therefore, effectively the decoder checks whether there exists a plausible set of input and output sequences at each relay that under the message w yield the observation $\mathbf{y}_d$. Given (11), note that the definition of consistency in (12) is closely related to weak typicality. Indeed, it is a variant of the weak typicality condition for Gaussian vectors. Therefore, effectively our decoder is a typicality decoder.

V. Error Analysis

An error occurs if the transmitted message w is not in the list, i.e., $w \notin \hat{\mathcal{W}}$ or when $w' \neq w$ is also in the list $\hat{\mathcal{W}}$. It is easy to show that the correct message w is in the list with high probability. We concentrate on the probability that there exist an error because w is not the unique message in $\hat{\mathcal{W}}$. This probability can be upper bounded by concentrating on the pair-wise error probabilities, i.e.,

$$P_e \le e^{nR}\,\mathbb{P}(w \to w')$$

where $\mathbb{P}(w \to w')$ is given by

$$\begin{aligned}&\mathbb{P}\left(\exists\{k_i'\}_{i\in\mathcal{N}} \text{ s.t.} (\mathbf{x}_s^{(w')}, \mathbf{y}_d, \{\tilde{\mathbf{y}}_i^{(k_i')}, \mathbf{x}_i^{(k_i')}\}_{i\in\mathcal{N}}) \in \widetilde{\mathcal{A}}_\epsilon\right) \\ &\qquad \le \sum_{k_1',\ldots,k_N'} \mathbb{P}\left((\mathbf{x}_s^{(w')}, \mathbf{y}_d, \{\tilde{\mathbf{y}}_i^{(k_i')}, \mathbf{x}_i^{(k_i')}\}_{i\in\mathcal{N}}) \in \widetilde{\mathcal{A}}_\epsilon\right)\end{aligned}$$

We can condition on the event that the correct message produces indices $\{k_i\}$, and since this is a generic index, we can carry out the entire calculation conditioned on this and then average over it. The summation over the N indices $k_1', \ldots, k_N'$ above can be rearranged to yield

$$\sum_{\Omega} \sum_{\substack{k_i', i\in\mathcal{N}_\Omega \\ k_i' \neq k_i}} \underbrace{\mathbb{P}\Big((\mathbf{x}_s^{(w')}, \mathbf{y}_d, \{\tilde{\mathbf{y}}_i^{(k_i')}, \mathbf{x}_i^{(k_i')}\}_i) \in \widetilde{\mathcal{A}}_\epsilon \text{ s.t. } k_i' = k_i, i \in \mathcal{N}_\Omega^c\Big)}_{\mathcal{P}}$$

where Ω is a source-destination cut of the network, i.e, $\Omega = \{s, \mathcal{N}_\Omega\}$ where $\mathcal{N}_\Omega$ is a subset of the relaying nodes $\mathcal{N}$. The first summation runs over all possible source-destination cuts Ω of the network, or equivalently over all subsets $\mathcal{N}_\Omega$ of the relaying nodes $\mathcal{N}$. Following [1], the rearrangement of the summation above can be interpreted as introducing a notion of distinguishability. The relay nodes in Ω are the ones that can distinguish between w and w' because $\tilde{\mathbf{y}}_i^{(k_i')} \neq \tilde{\mathbf{y}}_i^{(k_i)}$, when the relay nodes in Ω^c cannot distinguish between w and w' because $\tilde{\mathbf{y}}_i^{(k_i')} = \tilde{\mathbf{y}}_i^{(k_i)}$. The source node is naturally in the distinguishability set Ω and the destination node is in Ω^c. Thus, we sum over all possible cases for the distinguishability set Ω.

Now, let us examine the probability denoted by $\mathcal{P}$. For a given set of $\{k_i'\}_{i\in\mathcal{N}}$ such that $k_i' = k_i$, $i \in \mathcal{N}_\Omega^c$ and $k_i' \neq k_i$, $i \in \mathcal{N}_\Omega$, the consistency condition in (12) takes two different forms depending on whether $i \in \mathcal{N}_\Omega$ or $i \in \Omega^c$. For nodes $i \in \Omega^c$, the condition is equivalent to

$$\|(\sum_{j\in\Omega_{l-1}} h_{ij}(\mathbf{x}_j^{(k_j)} - \mathbf{x}_j^{(k_j')}) + \mathbf{z}_i - \mathbf{u}_i') \mod \Lambda^Q\|^2 \le n\,\sigma_c^2 \tag{13}$$

where $\Omega_{l-1} = \Omega \cap \mathcal{N}_{l-1}$ and we denote this event by $\mathcal{A}_i$. For nodes $i \in \mathcal{N}_\Omega$, the condition yields

$$\|(\tilde{\mathbf{y}}_i^{(k_i')} - \sum_{j\in\Omega_{l-1}^c} h_{ij}\mathbf{x}_j^{(k_j)} - \sum_{j\in\Omega_{l-1}} h_{ij}\mathbf{x}_j^{(k_j')}) \bmod \Lambda^Q\|^2 \le n\,\sigma_c^2 \tag{14}$$

where $\Omega_{l-1}^c = \Omega^c \cap \mathcal{N}_{l-1}$ and we denote this event by $\mathcal{B}_i$. We have,

$$\begin{aligned}\mathcal{P} &= \mathbb{P}\left(\{\mathcal{A}_i, i \in \Omega^c\}, \{\mathcal{B}_i, i \in \mathcal{N}_\Omega\}\right) \\ &= \mathbb{P}\left(\mathcal{A}_i, i \in \Omega^c\right) \mathbb{P}\left(\mathcal{B}_i, i \in \mathcal{N}_\Omega \,|\, \mathcal{A}_i, i \in \Omega^c\right).\end{aligned}$$

Note that due to Proposition 4.1, $\mathbf{x}_j^{(k_j)}, \mathbf{x}_j^{(k_j')}, j \in \{s, \mathcal{N}\}$ in expressions (13) and (14) are a set of independent random variables, uniformly distributed over $p_r^{-1}\Lambda^T \cap \mathcal{V}^T$. Due to the dithering in (10), $\tilde{\mathbf{y}}_i^{(k_i')}$ in (14) is uniformly distributed over the Voronoi region $\mathcal{V}_1^Q$ of the quantization lattice point $\hat{\mathbf{y}}_i^{(k_i')}$.

We will first bound the probability $\mathbb{P}\left(\mathcal{A}_i, i \in \Omega^c\right)$ by conditioning on the event defined in the following lemma.

Lemma 5.1: Let us define $\mathcal{E}_1$ to be the following event,

$$\Big\{\exists i \in \{\mathcal{N}, d\}, \exists \{k_j, k_j'\} \text{ s.t.} \sum_j h_{ij}(\mathbf{x}_j^{(k_j)} - \mathbf{x}_j^{(k_j')}) + \mathbf{z}_i - \mathbf{u}_i' \notin \mathcal{V}^Q\Big\}.$$

We have $\mathbb{P}(\mathcal{E}_1) \to 0$.

When $\mathcal{E}_1$ is true, we declare this as an error. This adds a vanishing term to the decoding error probability by the above lemma. Conditioning on the complement of $\mathcal{E}_1$ allows us to get rid of the mod operation w.r.t Λ^Q in (13). Given $\mathcal{E}_1^c$, the condition $\mathcal{A}_i$ is equivalent to

$$\mathcal{A}_i' = \big\{\|(\sum_{j \in \Omega_{l-1}} h_{ij}(\mathbf{x}_j^{(k_j)} - \mathbf{x}_j^{(k_j')}) + \mathbf{z}_i - \mathbf{u}_i')\|^2 \le n\,\sigma_c^2\big\}.$$

Therefore, we have

$$\mathbb{P}\left(\mathcal{A}_i, i \in \Omega^c \,|\, \mathcal{E}_1^c\right) = \mathbb{P}\left(\mathcal{A}_i', i \in \Omega^c \,|\, \mathcal{E}_1^c\right) \le \frac{\mathbb{P}\left(\mathcal{A}_i', i \in \Omega^c\right)}{\mathbb{P}(\mathcal{E}_1^c)}$$

We upperbound the last probability above in the following lemma.

Lemma 5.2:

$$\mathbb{P}\Big(\|\sum_{j \in \Omega_{l-1}} h_{ij}(\mathbf{x}_j^{(k_j)} - \mathbf{x}_j^{(k_j')}) + \mathbf{z}_i - \mathbf{u}_i'\|^2 \le n\,\sigma_c^2,\, \forall i \in \Omega^c\Big) \le e^{-n\left(I(X_\Omega; HX_\Omega + Z_{\Omega^c}) - \frac{1}{2}|\Omega^c|(1+\log(1+\epsilon)) - o_n(1)\right)},$$

where $X_i, i \in \Omega$ are i.i.d Gaussian random variables $\mathcal{N}(0, P)$, Z_{Ω^c} are i.i.d Gaussian random variables $\mathcal{N}(0, \sigma^2)$ and H is the channel transfer matrix from nodes in Ω to nodes in Ω^c.

The proof of the lemma involves two main steps. Recall that $\mathbf{x}_j^{(k_j)}, \mathbf{x}_j^{(k_j')}, j \in \Omega$ are discrete random variables, independently and uniformly distributed over $p_r^{-1}\Lambda^T \cap \mathcal{V}^T$. We first show that the probability in the lemma is upper bounded by

$$e^{n\epsilon_2}\mathbb{P}\Big(\|\sum_{j \in \Omega_{l-1}} h_{ij}(\mathbf{x}_j - \mathbf{x}_j') + \mathbf{z}_i - \mathbf{z}_i'\|^2 \le n\,\sigma_c^2,\, \forall i \in \Omega^c\Big) \tag{15}$$

where $\mathbf{x}_j, \mathbf{x}_j', j \in \Omega$ and $\mathbf{z}_i', i \in \Omega^c$ are all independent Gaussian random variables such that $\mathbf{x}_j, \mathbf{x}_j' \sim \mathcal{N}(0, \sigma_x^2 I_n)$, $\mathbf{z}_i' \sim \mathcal{N}(0, \sigma_z^2 I_n)$ and as n increases, $\sigma_x^2 \to \sigma^2(\Lambda^T) \to P$ if Λ^T is Roger's good, $\sigma_z^2 \to \sigma^2(\Lambda_1^Q) \to \sigma^2$ if Λ_1^Q is Roger's good which is our case here. $\epsilon_2 \to 0$ when $n \to \infty$, again if Λ^T and Λ_1^Q are Roger's good. Given this translation to Gaussian distributions the problem becomes very similar to the one for Gaussian codebooks in [1]. The second step is to bound the probability in (15) by following a similar approach to [1].

We will now upper bound the term

$$\sum_{\substack{k_i', i \in \mathcal{N}_\Omega \\ k_i' \neq k_i}} \mathbb{P}\left(\mathcal{B}_i, i \in \mathcal{N}_\Omega \,|\, \mathcal{A}_i, i \in \Omega^c\right) \tag{16}$$

by first removing the condition $k_i' \neq k_i$ in the summation above and then noting that this term is equal to $e^{|\mathcal{N}_\Omega| n R_r}$ times the probability $\mathbb{P}\left(\mathcal{B}_i, i \in \mathcal{N}_\Omega \,|\, \mathcal{A}_i, i \in \Omega^c\right)$ evaluated for a randomly and independently chosen set of indices $\{k_i'\}_{i \in \mathcal{N}_\Omega}$. When each of the indices $\{k_i'\}_{i \in \mathcal{N}_\Omega}$ is chosen uniformly at random, $\tilde{\mathbf{y}}_i^{(k_i')}$ in (14) is a random variable uniformly distributed over $\mathcal{V}^Q$. This is due to the dithering over the Voronoi region $\mathcal{V}_1^Q$ of the fine lattice and the mod operation with respect to the coarse lattice Λ^Q in (10). Moreover, by the Crypto Lemma,

$$\nu_i = \tilde{\mathbf{y}}_i^{(k_i')} - \sum_{j \in \Omega_{l-1}^c} h_{ij}\mathbf{x}_j^{(k_j)} - \sum_{j \in \Omega_{l-1}} h_{ij}\mathbf{x}_j^{(k_j')} \mod \Lambda^Q$$

is also uniformly distributed over $\mathcal{V}^Q$ and is independent of

$$\sum_{j \in \Omega_{l-1}^c} h_{ij}\mathbf{x}_j^{(k_j)} + \sum_{j \in \Omega_{l-1}} h_{ij}\mathbf{x}_j^{(k_j')}.$$

This is due to the fact that $\tilde{\mathbf{y}}_i^{(k_i')}$ is independent of this term, which is due to the fact the index k_i' and the dither $\mathbf{u}_i$ are chosen independently of everything else. Therefore (16) is upper bounded by

$$\begin{aligned}\sum_{k_i', i \in \mathcal{N}_\Omega} &\mathbb{P}\left(\mathcal{B}_i, i \in \mathcal{N}_\Omega \,|\, \mathcal{A}_i, i \in \Omega^c\right) \\ &= e^{|\mathcal{N}_\Omega| n R_r} \prod_{i \in \mathcal{N}_\Omega} \mathbb{P}\left(\|\nu_i\|^2 \le n\sigma_c^2\right) \\ &\le e^{|\mathcal{N}_\Omega| n \frac{1}{2}(\log(2(1+\epsilon)) + 1 + o_n(1))}\end{aligned} \tag{17}$$

where the last inequality follows from the below lemma.[2]

Lemma 5.3: Let ν be uniformly distributed over $\mathcal{V}^Q$. We have,

$$\mathbb{P}\Big(\|\nu\|^2 \le n\,\sigma_c^2\Big) \le e^{-\frac{n}{2}\left(\log\left(1 + \frac{\sigma^2(\Lambda^Q)}{\sigma_c^2}\right) - 1 - o_n(1)\right)}.$$

Combining the results of Lemma 5.2 and (17), an considering the summation over all possible source-destination cuts proves the main result of this paper stated in Theorem 2.1.

REFERENCES

[1] S. Avestimehr, S. Diggavi and D. Tse, *Wireless network information flow: a deterministic approach*, eprint arXiv:0906.5394v2 - arxiv.org.

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

[3] G. Kramer, I. Maric, and R. Yates, *Cooperative Communications*. Foundations and Trends in Networking, 2006.

[4] B. Nazer and M. Gastpar, *Computation over Multiple Access Channels*,, IEEE Trans. on Information Theory, vol.53, no.10, pp.3498-3516, October 2007.

[5] W. Nam and S.-Y. Chung, *Relay networks with orthogonal components*, in Proc. 46th Annual Allerton Conference, Sept.2008.

[6] U. Erez and R. Zamir, *Achieving* $\frac{1}{2}\log(1+SNR)$ *on the AWGN channel with lattice encoding and decoding*, IEEE Trans. on Information Theory, vol.50, no.10, pp.2293-2514, Oct. 2004.

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

[8] H.-A. Loeliger, *Averaging bounds for lattices and linear codes*, IEEE Trans. on Information theory, vol.43, pp. 1767-1773, Nov. 1997.

[9] 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.

[10] A. Özgür and S. Diggavi, *Approximately achieving Gaussian relay network capacity with lattice codes*, e-print - arXiv.org, May 2010.

[2] An alternative way to upper bound (16) is to randomly choose the quantization lattices at each relay instead of using a fixed lattice.