

Structured Codes and Cooperative Strategies in Wireless Relay Networks

BY

YIWEI SONG

B.E. Nanjing University of Posts and Telecommunications, Nanjing, China, 2009

THESIS

Submitted as partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Chicago, 2013

Chicago, Illinois

Defense Committee:

Natasha Devroye, Chair and Advisor

Daniela Tuninetti

Rashid Ansari

Dan Schonfeld

Huai-Rong Shao, Samsung Information System America

TABLE OF CONTENTS

<u>CHAPTER</u>	<u>PAGE</u>
1 INTRODUCTION	1
1.1 Motivation and background	2
1.2 Related work	4
1.3 Contribution	9
2 MOTIVATIONAL EXAMPLES	12
2.1 Information theory and network information theory	12
2.2 Cooperative strategies	13
2.3 Structured codes	15
2.4 Wireless relay networks	17
3 PRELIMINARIES ON LATTICE CODES	19
3.1 Lattice codes	19
3.2 Nested lattice codes	23
3.3 Nested lattice chains	24
4 LATTICE CODING FOR DECODE-AND-FORWARD	25
4.1 Lattice list decoding	25
4.2 Decode-and-Forward for the AWGN single relay channel	33
4.3 Decode-and-Forward for the AWGN multi-relay channel	41
4.4 The AWGN two-way relay channel with direct links	43
4.4.1 Comparison to existing rate regions	53
4.5 The AWGN multiple-access relay channel	54
4.6 Lattice Dirty-Paper Coding in Simple Relay Channel	60
4.6.1 Channel Model	61
4.6.2 Lattice Achievability	63
5 LATTICE CODING FOR COMPRESS-AND-FORWARD IN SINGLE RELAY CHANNEL	69
5.1 Lattice codes for the Wyner-Ziv model in Compress-and-Forward	70
5.2 Lattice coding for Compress-and-Forward	75
6 LATTICE CODING FOR TWO-WAY TWO-RELAY CHANNEL	80
6.1 Simple but Special Lattice Codes for the Two-way Two-relay Channel	81
6.1.1 Construction	81
6.1.2 Technical lemmas	83

TABLE OF CONTENTS (Continued)

<u>CHAPTER</u>		<u>PAGE</u>
6.2	Channel Model	84
6.3	Lattice Codes in the BC Phase of the Two-way Relay Channel	86
6.4	The proposed protocol and achievable rates for the Two-way Two-relay channel	94
6.5	Extensions to half-duplex channels and more than two relays	104
6.5.1	Half-duplex	104
6.5.2	More than two relays	105
7	CONCLUSION	107
	APPENDICES	109
	CITED LITERATURE	119
	VITA	126

LIST OF FIGURES

<u>FIGURE</u>		<u>PAGE</u>
1	Three-node relay channel and Two-way relay channel	14
2	Decoding the sum of codewords	18
3	A lattice chain $\Lambda \subseteq \Lambda_s \subseteq \Lambda_c$ with corresponding fundamental regions $\mathcal{V} \supseteq \mathcal{V}_s \supseteq \mathcal{V}_c$ of volumes $V \geq V_s \geq V_c$. Color is useful.	20
4	The two equivalent lists, in this example consisting of the four points encircled in red. The correct message lattice point is the center. Color is useful.	28
5	The two Gaussian relay channels under consideration in Section 4.2 and Section 4.4. For the AWGN relay channel we have assumed a particular relay order (2,3) for our achievability scheme and shown the equivalent channel model used in deriving the achievable rate rather than the general channel model.	35
6	Lattice Decode-and-Forward scheme for the AWGN relay channel. . . .	36
7	The AWGN two-way relay channel with direct links and the AWGN multiple-access relay channel. We illustrate the lists $L_{i \rightarrow j}^w$ of messages w carried by the codewords at node i and list decoded according to Theorem 3 at node j	44
8	Lattice Decode-and-Forward scheme for the AWGN two-way relay channel with direct links.	47
9	Comparison of decode-and-forward achievable rate regions of various two-way relay channel rate regions.	55
10	Lattice Decode-and-Forward scheme for the AWGN multiple access relay channel.	57
11	Interference S is experienced at the destination but only known at the source.	62

LIST OF FIGURES (Continued)

<u>FIGURE</u>		<u>PAGE</u>
12	Illustration of key achievability steps: (a) interference “pre-cancellation” is performed at the transmitter Node 1 who knows the interference S , (b) the receiver Node 3 experiences interference S , and suffers from a quantization noise “residual”.	64
13	Lattice coding for the $(\mathbf{X} + \mathbf{Z}_1, \mathbf{X} + \mathbf{Z}_2)$ Wyner-Ziv problem.	72
14	The Gaussian Two-way Two-relay Channel Model.	84
15	Re-distribution Transform illustration for a one-dimensional lattice. . .	92
16	Multi-phase Block Markov achievability strategy for Theorem 19.	96
17	Half-duplex case.	106
18	Lattice Decode-and-Forward scheme for the AWGN multi-relay channel.	111
19	Multi-phase Block Markov achievability strategy for Lemma 20.	118

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
DF	Decode-and-Forward
CF	Compress-and-Forward
i.i.d.	independent and identically distributed
MAC	Multiple access channel
BC	Broadcast channel
IC	Interference channel
TWC	Two-way channel
RC	Relay channel

SUMMARY

Lattice codes are known to achieve capacity in the Gaussian point-to-point channel, thereby achieving the same rates as random Gaussian codebooks. Lattice codes are also known to outperform random codes for certain channel models that are able to exploit their linearity. In this thesis, we first show that lattice codes may be used to achieve the same performance as known Gaussian random coding techniques for the Gaussian relay channel. Then several examples are given to show how this may be combined with the linearity of lattices codes in multi-source relay networks. Finally we show that lattice codes's advantages in the two-way multi-hop Channel. In particular, we present a nested lattice list decoding technique, by which, lattice codes are shown to achieve the Decode-and-Forward (DF) rate of single source, single destination Gaussian relay channels with one or more relays. We next present a few examples of how this DF scheme may be combined with the linearity of lattice codes to achieve rates which may outperform analogous Gaussian random coding techniques in multi-source relay channels such as the two-way relay channel with direct links and the multiple access relay channel. We furthermore present a lattice Compress-and-Forward (CF) scheme which exploits a lattice Wyner-Ziv binning scheme for the Gaussian relay channel which achieves the same rate as the Cover-El Gamal CF rate using Gaussian random codes. Finally, the linearity of lattice codes is further utilized in two-way multi-hop channels where the "Redistribution Transform" is proposed to fully exploit the transmit power of relays for both directions. These

SUMMARY (Continued)

results suggest that structured/lattice codes may be used to mimic, and sometimes outperform, random Gaussian codes in general Gaussian networks.

CHAPTER 1

INTRODUCTION

The derivation of achievable rate regions for general networks including relays has classically used codewords and codebooks consisting of independent, identically generated symbols (i.i.d. random coding). Only in recent years have codes which possess additional structural properties, which we term structured codes, been used in networks with relays (1; 2; 3; 4; 5; 6; 7). The benefit of using structured codes in networks lies not only in a somewhat more constructive achievability scheme and possibly computationally more efficient decoding than i.i.d. random codes, but also in actual rate gains which exploit the structure of the codes – their linearity in Gaussian channels – to decode combinations of codewords rather than individual codewords / messages. While past work has focussed mainly on specific scenarios in which structured or lattice codes are particularly beneficial, missing is the demonstration that lattice codes may be used to achieve the same rate as known i.i.d. random coding based schemes in Gaussian relay networks, in addition to going above and beyond i.i.d. random codes in certain scenarios. In the first part of this work we demonstrate generic nested lattice code based schemes with computationally more efficient lattice decoding for achieving the Decode-and-Forward and Compress-and-Forward rates in Gaussian relay networks which achieve at least the same rate regions as the corresponding rates achieved using Gaussian random codes.

In the longer term, these strategies may be combined with ones which exploit the linear structure of lattice codes to obtain structured coding schemes for arbitrary Gaussian relay

networks. Towards this goal, we illustrate how the DF based lattice scheme may be combined with strategies which exploit the linearity of lattice codes in two examples: the two-way relay channel with direct links and the multiple-access relay channel.

Another example of utilizing linearity of lattice codes in the multi-source scenarios is the lattice coding for the Two-way Two-relay Channel $1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4$ where Node 1 and 4 simultaneously communicate with each other through two relay nodes 2 and 3. Each node only communicates with its neighboring nodes. This lattice coding scheme can be seen as a generalization of lattice coding scheme for Two-way Relay Channel (3; 2). Similarly, gains stem from the ability to decode the sum of codewords (or messages) using lattice codes at higher rates than possible with i.i.d. random codes. The key technical contribution is the lattice-based achievability strategy, where each relay is able to remove the noise while decoding the sum of several signals in a Block Markov strategy and then re-encode the signal into another lattice codeword using the so-called “Re-distribution Transform”. This allows nodes further down the line to again decode sums of lattice codewords. This transform is central to improving the achievable rates, and ensures that the messages traveling in each of the two directions fully utilize the relay’s power, even under asymmetric channel conditions. All decoders are lattice decoders and only a single nested lattice codebook pair is needed. The symmetric rate achieved by the proposed lattice coding scheme is within $\frac{1}{2} \log 3$ bit/Hz/s of the symmetric rate capacity.

1.1 Motivation and background

In relay networks, as opposed to single-hop networks, multiple links or routes exist between a given source and destination. Of key importance in such networks is how to best jointly uti-

lize these links, which – in a single source scenario – all carry the same message and effectively cooperate with each other to maximize the number of messages that may be distinguished. The three node relay channel with one source with one message for one destination aided by one relay is the simplest relay network where pure cooperation between the links is manifested. Information may flow along the direct link or along the relayed link; how to manage or have these links cooperate to best transmit this message is key to approaching capacity for this channel. Despite this network’s simplicity, its capacity remains unknown in general. However, the following two “cooperative” achievability schemes may approach capacity under specific channel conditions: “Decode-and-Forward” (DF) and “Compress-and-Forward” (CF) strategies described in (8; 9; 10; 11). In the DF scheme, the receiver does not obtain the entire message from the direct link nor the relayed link. Rather, cooperation between the direct and relayed links may be implemented by having the receiver decode a list of possible messages (or codewords) from the direct link, another independent list from the coherent combination of the direct link and the relayed link, which it then intersects to obtain the message sent¹. In the CF scheme of (8), cooperation is implemented by a two-step decoding procedure combined with Wyner-Ziv binning.

Generalizations of these i.i.d. random-coding based DF and CF schemes have been proposed for general multi-terminal relay networks (9; 12; 13). However, in recent years lattice codes have been shown to outperform random codes in several Gaussian multi-source network scenarios

¹There are alternative schemes for implementing DF, but the main intuition about combining information along two paths remains the same.

due to their linearity property (1; 14; 15; 2; 3; 4). As such, one may hope to derive a coding scheme which combines the best of both worlds, i.e. incorporate lattice codes with their linearity property into coding schemes for general Gaussian networks. At the moment we cannot simply replace i.i.d. random codes with lattice codes. That is, while nested lattice codes have been shown to be capacity achieving in the point-to-point Gaussian channel, in relay networks with multiple links/paths and the possibility of cooperation, technical issues need to be solved before one may replace random codes with lattice codes.

In this thesis, we make progress in this direction by demonstrating lattice-based cooperative techniques for a number of relay channels. One of the key new technical ingredients in the DF schemes is the usage of a lattice list decoding scheme to decode a list of lattice points (using lattice decoding) rather than a single lattice point. We then extend this lattice-list-based cooperative technique and combine it with the linearity of lattice codes to provide gains for some channel conditions over i.i.d. random codes in scenarios with multiple cooperating links. Finally, the Re-distribution Transform is utilized to fully exploit the transmit power of relay nodes in the Two-way Two-relay Channel.

1.2 Related work

In showing that lattice codes may be used to replace i.i.d. random codes in Gaussian relay networks and introducing the novel lattice coding scheme for Two-way Two-relay Channel, we build upon work on relay channels, on the existence of “good” nested lattice codes for Gaussian source and channel coding, and on recent advancements in using lattices in multiple-relay and multiple-node scenarios. We outline the most relevant related work.

Relay channels. Two of our main results are the demonstration that nested lattice codes may be used to achieve the DF and CF rates achieved by random Gaussian codes (8). For the DF scheme, we mimic the Regular encoding/Sliding window decoding DF strategy (9; 10) in which the relay decodes the message of the source, re-encodes it, and then forwards it. The destination combines the information from the source and the relay by intersecting two independent lists of messages obtained from the source and relayed links respectively, over two transmission blocks. We will re-derive the DF rate, but with lattice codes replacing the random i.i.d. Gaussian codes. Of particular importance is constructing and utilizing a lattice version of the list decoder. It is worth mentioning that the concurrent work (6) uses a different lattice coding scheme to achieve the DF rate in the three-node relay channel which does not rely on list decoding but rather on a careful nesting structure of the lattice codes.

The DF scheme of (8) restricts the rate by requiring the relay to decode the message. The Compress-and-Forward (CF) achievability scheme of (8) for the relay channel places no such restriction, as the relay compresses its received signal and forwards the compression index. In Cover and El Gamal's original CF scheme, the relay's compression technique utilizes a form of binning related to the Wyner-Ziv rate-distortion problem with decoder side-information (16). In (17; 18) the authors describe a lattice version of the noiseless quadratic Gaussian Wyner-Ziv coding scheme, where lattice codes quantize/compress the continuous signal; this will form the basis for our lattice-based CF strategy. Another simple structured approach to the relay channel is considered in (19; 20) where one-dimensional structured quantizers are used in the relay channel subject to instantaneous (or symbol-by-symbol) relaying.

Our extension of the single relay DF rate to a multiple relay DF rate is based on the DF multi-level relay channel scheme presented in (12; 9). These papers essentially extend the DF rate of (8); the central idea behind mimicking the scheme of (9; 12) is the repeated usage of the lattice list decoder, enabling the message to again be decoded from the intersection of multiple independent lists formed at the destination from the different relay - destination links.

This work also considers the Two-way Two-relay Channel: $1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4$ where two user Nodes 1 and 4 exchange information with each other through the relay nodes 2 and 3. This is related to the work of (21), which considers the throughput of i.i.d. random code-based Amplify-and-Forward and Decode-and-Forward approaches for this channel model, or the i.i.d. random coding based schemes of (22) and (23) where there are furthermore links between all nodes. This model is also different from that in (24) where a two-way relay channel with two *parallel* (rather than sequential as in this work) relays are considered.

Lattice codes for single-hop channels. Lattice codes are known to be “good” for almost everything in Gaussian point-to-point, single-hop channels (25; 26; 27), from both source and channel coding perspectives. In particular, nested lattice codes have been shown to be capacity achieving for the AWGN channel, the AWGN broadcast channel (18) and the AWGN multiple access channel (1). Lattice codes may further be used in achieving the capacity of Gaussian channels with interference or state known at the transmitter (but not receiver) (28) using a lattice equivalent (18) of dirty-paper coding (DPC) (29). The nested lattice approach of (18) for the dirty-paper channel is extended to dirty-paper networks in (30), where in some scenarios lattice codes are interestingly shown to outperform random codes. In $K \geq 3$ -user interference

channels, their structure has enabled the decoding of (portions of) “sums of interference” terms (14; 15; 31; 32), allowing receivers to subtract off this sum rather than try to decode individual interference terms in order to remove them. From a source coding perspective, lattices have been useful in distributed Gaussian source coding when reconstructing a linear function (33; 34).

Lattice codes in multi-hop channels. The linearity property of lattice codes have been exploited in the Compute-and-Forward framework (1) for Gaussian multi-hop wireless relay networks (2; 3; 4). There, intermediate relay nodes decode a linear combination, or equation, of the transmitted codewords or equivalently messages by exploiting the noisy linear combinations provided by the channel. Through the use of nested lattice codes, it was shown that decoding linear combinations may be done at higher rates than decoding the individual codewords – one of the key benefits of using structured rather than i.i.d. random codewords (35). Recently, progress has been made in characterizing the capacity of a single source, single destination, multiple relay network to within a constant gap for arbitrary network topologies (36). Capacity was initially shown to be approximately achieved via an i.i.d. random quantize-map-and-forward based coding scheme (36) and alternatively, using an extension of CF based techniques termed “noisy network coding” (13). Recently, relay network capacity was also shown to be achievable using nested lattice codes for quantization and transmission (5). Alternatively, using a new “computation alignment” scheme which couples lattice codes in a compute-and-forward-like framework (1) together with a signal-alignment scheme reminiscent of ergodic interference alignment (37), the work (38) was able to show a capacity approximation for multi-layer wireless relay networks with an approximation gap that is independent of the network depth. While

lattices have been used in relay networks, the goals so far have mainly been to demonstrate their utility in specific networks in which decode linear combinations of messages is beneficial, or to achieve finite-gap results.

As a first example of the use of lattices in multi-hop scenarios, we will consider the Gaussian two-way relay channel (3; 2). The two-way relay channel consists of three nodes: two terminal nodes 1 and 2 that wish to exchange their two independent messages through the help of one relay node R. When the terminal nodes employ *nested lattice codes*, the sum of their signals is again a lattice point and may be decoded at the relay. Having the relay send this sum (possibly re-encoded) allows the terminal nodes to exploit their own message side-information to recover the other user's message (2; 3). Gains over DF schemes where both terminals transmit simultaneously to the relay stem from the fact that, if using random Gaussian codebooks, the relay will see a multiple-access channel and require the decoding of both individual messages, even though the sum is sufficient. In contrast, no multiple-access (or sum-rate) constraint is imposed by the lattice decoding of the sum. An alternative non-DF (hence no rate constraints at relay) yet still structured approach to the two-way relay channel is explored in (39; 40), where simple one dimensional structured quantizers are used for a symbol-by-symbol Amplify-and-Forward based scheme. In the two-way relay channel, models with and without direct links between the transmitters have been considered. While random coding techniques have been able to exploit both the direct link and relayed links, lattice codes have only been used in channels without direct links. Here, we will present a lattice coding scheme which will combine the

linearity properties, leading to less restrictive decoding constraints at the relay, with direct-link information, allowing for a form of lattice-enabled two-way cooperation.

A second example in which we will combine the linearity property with direct-link cooperation is the Gaussian multiple-access relay channel (41; 10; 42). In this model, two sources wish to communicate independent messages to a common destination with the help of a single relay. As in the Gaussian two-way relay channel, the relay may choose to decode the sum of the codewords using lattice codes, rather than the individual codewords (as in random coding based DF schemes), which it would forward to the destination. The destination would combine this sum with direct-link information (cooperation). As in the two-way relay channel, decoding the sum at the relay eliminates the multiple access sum-rate constraint.

Finally, the linearity of lattice codes is extended to Two-way Two-relay Channel where two sources communicate with each other through two relays (two relays). As in the previous examples, the relays will decode the sum of two codewords and forward this appropriately scaled and transformed sum. The difference is that the relay nodes need to forward (broadcast) the decoded sum using lattice codes in order to again “decode the sum” down the line. A specially designed lattice coding strategy is used in this example to enable broadcasting with lattice codes while at the same time dealing with power asymmetry of the two received signals, something which had previously not been tackled.

1.3 Contribution

The contributions center around demonstrating the lattice coding scheme in the wireless relay networks. We aim to show that lattices may achieve the same rates as currently known

Gaussian i.i.d. random coding-based achievability schemes for relay networks. While we do not prove this sweeping statement in general, we make progress towards this goal along the following lines. The linearity is also combined with cooperation strategies we developed in multi-source scenarios. Moreover, we extend the linearity to Two-way Two-relay Channel, in which the key technique “Redistribution Transform” is proposed.

- **Preliminaries:** In Chapter 3 we briefly outline lattice coding preliminaries and notation before outlining key technical lemmas that will be needed.
- **Lattice list decoding and Decode-and-Forward, single source:** One of the central contributions, the proposed Lattice List Decoding technique in Theorem 3 is proved in Chapter 4.1. This Lattice List Decoding technique is used to show that nested lattice codes may achieve the Decode-and-Forward rate for the Gaussian relay channel achieved by i.i.d. random Gaussian codes (8) in Chapter 4.2, Theorem 7. We furthermore extend this result to the general single source, multiple relay Gaussian channel in Theorem 8.
- **Decode-and-Forward, multiple source including two-way relay and multiple access relay channels:** In Chapter 4.4 and 4.5, relays decode and forward combinations of messages as in the Compute-and-Forward framework, which is combined with direct link side-information at the destination. In particular, we present lattice-based achievable rate regions for the Gaussian two-way relay channel with direct links in Theorem 9, and the Gaussian multiple-access relay channel in Theorem 10.
- **Compress-and-Forward, single source:** In Chapter 5, we revisit our goal of showing that lattice codes may mimic the performance of i.i.d. Gaussian codes in the relay chan-

nel by demonstrating a lattice code-based Compress-and-Forward scheme which achieves the same rate as the CF scheme in (8) evaluated for i.i.d. Gaussian codebooks. The proposed lattice CF scheme is based on a variation of the lattice-based Wyner-Ziv scheme of (17; 18), as outlined in Theorem 13. We note that lattices have been shown to achieve the Quantize-Map-and-Forward rates for general relay channels using Quantize-and-Map scheme (similar to the CF scheme) which simply quantizes the received signal at the relay and re-encodes it without any form of binning / hashing in (5); the contribution is to show an alternative lattice-coding based achievability scheme which employs computationally more efficient lattice decoding.

- **Two-way Two-relay Channel:** In Chapter 6, a novel lattice coding scheme is proposed for the Two-way Two-relay Channel. The key technical contribution is the lattice-based achievability strategy, where each relay is able to remove the noise while decoding the sum of several signals in a Block Markov strategy and then re-encode the signal into another lattice codeword using the so-called “Re-distribution Transform”. This allows nodes further down the line to again decode sums of lattice codewords. This transform is central to improving the achievable rates, and ensures that the messages traveling in each of the two directions fully utilize the relay’s power, even under asymmetric channel conditions. All decoders are lattice decoders and only a single nested lattice codebook pair is needed. The achievability scheme is proved in Theorem 19 and 21. The symmetric rate achieved by the proposed lattice coding scheme is within $\frac{1}{2} \log 3$ bit/Hz/s of the symmetric rate capacity.

CHAPTER 2

MOTIVATIONAL EXAMPLES

This chapter outlines and motivates our work with several examples, in order to develop an initial intuitive understanding of this work. We first explain the three key topics/ideas explored in this thesis: cooperative strategies, structured codes, and wireless relay networks.

2.1 Information theory and network information theory

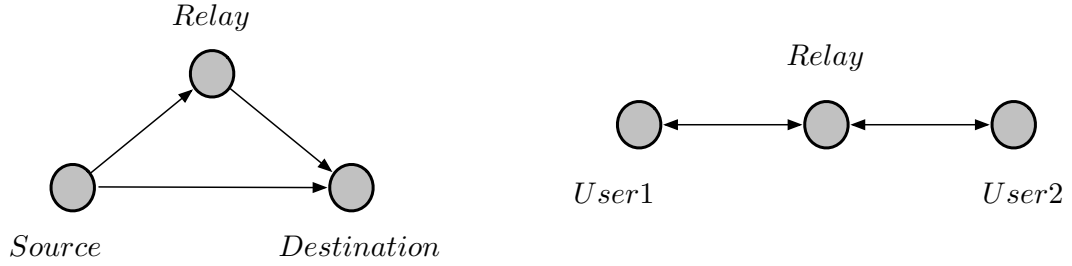
Information theory originates from Shannon’s seminal paper (43), which proposed a mathematical model for point-to-point communication channel and defined the maximum reliable transmission rate as that channel’s “capacity”. The capacity of a point-to-point channel is determined as $C = \max_{p(x)} I(X; Y) = \max_{p(x)} H(X) - H(X|Y)$, where $H(X)$ represents the “uncertainty” before transmission and $H(X|Y)$ represents the “uncertainty” after transmission. Intuitively, $\max_{p(x)} I(X; Y) = H(X) - H(X|Y)$ can be understood as the “uncertainty” resolved in the channel. The capacity of the additive white Gaussian noise (AWGN) channel is $C = \frac{1}{2} \log(1 + SNR)$ bits/transmission where SNR is the signal to noise ratio.

While Shannon determined the capacity of the point-to-point channel, there are many other open problems in the network information theory where the communications models are more than just point-to-point channel. Progress has been made in obtaining the capacity region for several simpler network models. The multiple access channel (MAC) describes a scenario where multiple users send messages to one receiver at the same time. The capacity region of

this model is completely known, giving information theorists hopes of generalizing Shannon’s model to arbitrary networks. In a broadcast channel (BC), a single transmitter sends multiple messages to multiple receivers at the same time. The capacity of the BC is generally unknown but the AWGN broadcast channel’s capacity was recently solved. The interference channel (IC) describes a scenario where two pairs of transmitters and receivers communicate at the same time and interfere with each other. The capacity of the IC has remained open for decades, even for the AWGN channel. The two-way channel (TWC) represents a scenario where two users communicate with each other simultaneously. The capacity is generally unknown but the AWGN case is simple since the two-way AWGN channel may be shown to decompose into two independent point-to-point channels, whose capacities are known. A relay channel (RC) describes the cooperation phenomenon in wireless networks, where the same message may be transmitted along various paths, and will be explained in the next section. An elegant introduction and more detailed explanations can be found at (44; 11). These channel models not only characterize the specific model they describe, but also correspond to communication phenomena in the real world, e.g. the MAC may correspond to the uplink of a wireless communication system, the BC the downlink.

2.2 Cooperative strategies

We use “cooperative strategies” to mean wireless cooperative strategies in relay networks where there are multiple wireless links between the source and destination. How to cooperatively utilize these links to approach the capacity are called cooperative strategies. This section introduces two popular cooperative strategies: Decode-and-Forward(DF) and Compress-and-



Three-node relay channel

Two-way relay channel without direct links

Figure 1. Three-node relay channel and Two-way relay channel

Forward(CF) with the simplest relay channel: three-node relay channel, where the transmitter communicates with the destination with a help of relay as shown in Figure 1. The broadcast and interference nature of the wireless channel are shown in this example: both the relay and the destination observe the same signal sent by the source, and the signals sent by the relay and source interfere with each other at the destination. The capacity of this channel has remained open for decades and hence the optimal cooperative strategy remains unknown. Two popular strategies are:

Decode-and-Forward: As the name indicates that, the relay is required to decode the message and cooperatively forwards the message to the destination. Thus, after the relay decodes the message, the model becomes a cooperative multiple access channel: both relay and source send the same message to the destination cooperatively. Specifically, the destination can decode two lists from the source-destination link and relay-destination link respectively

and intersects these two lists to obtain the desired unique codeword. The problem with this strategy is that the relay *must* decode the message, which is not necessary intuitively. However, when the source-relay link is very strong, decoding the message is a reasonable thing for the relay to do. Specifically, there are three different achievability schemes which achieves the same DF rate region, which are described in (10). But they all have the same intuition described above.

Compress-and-Forward: In this scheme, the relay does not have to decode the message. Instead, it treats its received signal as randomly generated and quantizes it. It then forwards the a function of the quantization index to the destination and the destination decodes the message from direct link and quantization index cooperatively. In its current form, the relay does not utilize codebook structure and so intuitively CF may be able to be improved upon through exploiting codebook structure.

To summarize, DF exploits the codebook structure at the relay but has to decode the message while CF does not have to decode the message but ignore the codebook structure. Intuition suggests that the optimal strategy may utilize the codebook structure but does not necessarily decode the message. However, no such schemes currently exist.

2.3 Structured codes

“Structured codes” may refer to codes with some form of structural property (often algebraic), but in this thesis we use it synonymously with lattice codes, which are structured codes well suited to the practically motivated AWGN channels. An excellent example to demonstrate the advantages of such structured lattice codes is the AWGN two-way relay channel, where two

sources exchange information through a relay as shown in figure Figure 1. The channel model between transmitters and the relay can be expressed as

$$\mathbf{Y}_R = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}_R$$

$$\mathbf{Y}_1 = \mathbf{X}_R + \mathbf{Z}_1$$

$$\mathbf{Y}_2 = \mathbf{X}_R + \mathbf{Z}_2$$

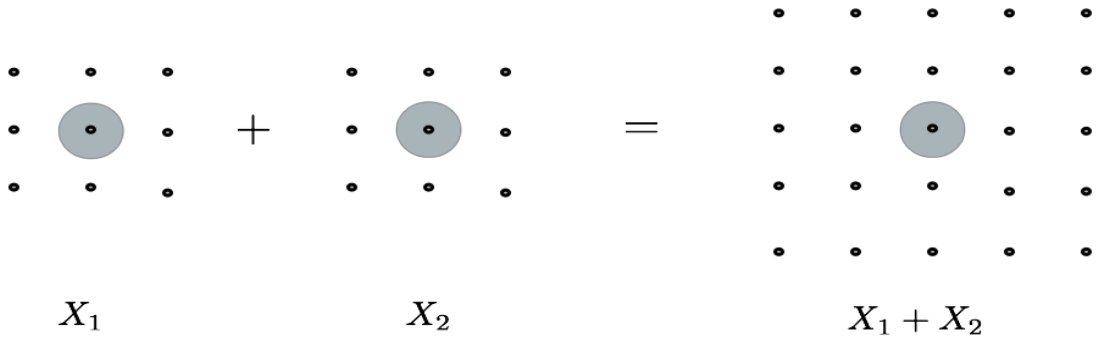
where \mathbf{X}_1 , \mathbf{X}_2 and \mathbf{X}_R represent the transmitted signals sent by two users and the relay respectively, $\mathbf{Y}_1, \mathbf{Y}_2$ and \mathbf{Y}_R represent the received signals by two users and the relay respectively, and $\mathbf{Z}_1, \mathbf{Z}_2$ and \mathbf{Z}_R are i.i.d. Gaussian noise. This model is full-duplex, which means both users and the relay are transmitting and receiving at the same time.

One possible transmission scheme is the following: the relay decodes both messages as in the multiple access channel (MAC) and subsequently broadcasts the two messages as in the broadcast channel (BC). However, we notice that it is not necessary for the relay to decode both messages individually since both users can decode the desired information from the sum of the codewords $\mathbf{X}_1 + \mathbf{X}_2$ with their own message as side information. It is intuitive to observe that decoding $\mathbf{X}_1 + \mathbf{X}_2$ should be “easier” than decoding $(\mathbf{X}_1, \mathbf{X}_2)$ since knowledge of $(\mathbf{X}_1, \mathbf{X}_2)$ allows one to obtain $\mathbf{X}_1 + \mathbf{X}_2$ but not vice-versa (there is more information in the pair of codewords than in their sum). However, it turns out that decoding $\mathbf{X}_1 + \mathbf{X}_2$ is equivalent to decoding $(\mathbf{X}_1, \mathbf{X}_2)$ if random codes are used as shown in Figure 2. However, this is not true for structured, or linear codes, where the space between codewords sums $\mathbf{X}_1 + \mathbf{X}_2$ is much larger

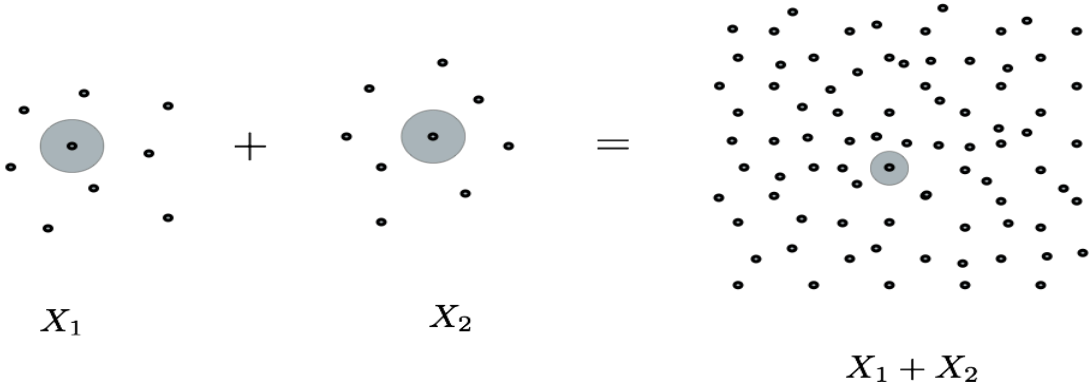
(than that with random codes), which means we can pack in more codewords for higher rate given the same noise. In other words, decoding $\mathbf{X}_1 + \mathbf{X}_2$ with linear codes is less constraining, in terms of rate, or number of pairs that may be resolved, than with random codes.

2.4 Wireless relay networks

To determine the capacity of an arbitrary wireless network is the ultimate goal of network information theory. Because of the broadcast and interference nature of the wireless channel, this problem turns out to be extremely difficult. Cooperative strategies and interference management (or exploitation) are two of the most important aspects of wireless networks. This thesis focuses on the cooperative strategies achievable using lattice codes. The advantage of lattice codes over random codes is shown above, in decoding the “sums” of codewords. However, whether lattice codes can replace random codes in AWGN relay networks in general to achieve a better rate region remains unclear. To replace random codes with lattice codes, lattice codes need to be shown to at least achieve the same performance as random codes. In some cases then, one may further exploit their linearity to outperform current known random coding based achievability schemes.



Decoding the sum with structure codes



Decoding the sum with random codes

Figure 2. Decoding the sum of codewords

CHAPTER 3

PRELIMINARIES ON LATTICE CODES

We introduce our notation for lattice codes, nested lattice codes, and nested lattice chains and present several existing lemmas.

3.1 Lattice codes

Our notation for (nested) lattice codes for transmission over AWGN channels follows that of (18; 4); comprehensive treatments may be found in (45; 18; 25) and in particular (27). An n -dimensional lattice Λ is a discrete subgroup of Euclidean space \mathbb{R}^n with Euclidean norm $\|\cdot\|$ under vector addition and may be expressed as all integral combinations of basis vectors $\mathbf{g}_i \in \mathbb{R}^n$

$$\Lambda = \{\lambda = G \mathbf{i} : \mathbf{i} \in \mathbb{Z}^n\},$$

for \mathbb{Z} the set of integers, $n \in \mathbb{Z}_+$, and $G := [\mathbf{g}_1 | \mathbf{g}_2 | \cdots | \mathbf{g}_n]$ the $n \times n$ generator matrix corresponding to the lattice Λ . We use bold \mathbf{x} to denote column vectors, \mathbf{x}^T to denote the transpose of the vector \mathbf{x} . All vectors are generally in \mathbb{R}^n unless otherwise stated, and all logarithms are base 2. Let $\mathbf{0}$ denote the all zeros vector of length n , \mathbf{I} denote the $n \times n$ identity matrix, and $\mathcal{N}(\mu, \sigma^2)$ denote a Gaussian random variable (or vector) of mean μ and variance σ^2 . Define $C(x) := \frac{1}{2} \log_2(1+x)$. Further define

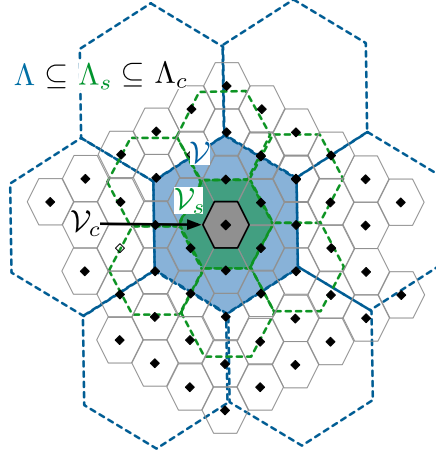


Figure 3. A lattice chain $\Lambda \subseteq \Lambda_s \subseteq \Lambda_c$ with corresponding fundamental regions $\mathcal{V} \supseteq \mathcal{V}_s \supseteq \mathcal{V}_c$ of volumes $V \geq V_s \geq V_c$. Color is useful.

- The *nearest neighbor lattice quantizer* of Λ as

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

- The $\bmod \Lambda$ operation as $\mathbf{x} \bmod \Lambda := \mathbf{x} - Q(\mathbf{x})$;
- The *fundamental Voronoi region* of Λ as the points closer to the origin than to any other

lattice point

$$\mathcal{V} := \{\mathbf{x} : Q(\mathbf{x}) = \mathbf{0}\},$$

which is of volume $V := \text{Vol}(\mathcal{V})$ (also sometimes denoted by $V(\Lambda)$ or V_i for lattice Λ_i);

- The *second moment per dimension* of a uniform distribution over \mathcal{V} as

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

- The *normalized second moment* of a lattice Λ of dimension n as

$$G(\Lambda) := \frac{\sigma^2(\Lambda)}{V^{2/n}};$$

- A sequence of n -dimensional lattices $\Lambda^{(n)}$ is said to be *Poltyrev good* (46; 25; 4) (in terms of channel coding over the AWGN channel) if, for $Z \sim \mathcal{N}(0, \bar{\sigma}^2 \mathbf{I})$ and n -dimensional vector, we have

$$\Pr\{Z \notin \mathcal{V}^{(n)}\} \leq e^{-n(E_P(\mu) - o_n(1))},$$

which upper bounds the error probability of nearest lattice point decoding when using lattice points as codewords in the AWGN channel. Here $E_p(\mu)$ is the *Poltyrev exponent* (25; 47) which is given as

$$E_p(\mu) = \begin{cases} \frac{1}{2}[(\mu - 1) - \log \mu], & 1 < \mu \leq 2 \\ \frac{1}{2} \log \frac{e\mu}{4} & 2 \leq \mu \leq 4, \\ \frac{\mu}{8} & \mu \geq 4. \end{cases}$$

and μ is volume-to-noise ratio (VNR) defined as (26)

$$\mu := \frac{(\text{Vol}(\mathcal{V}))^{2/n}}{2\pi e \bar{\sigma}^2} + o_n(1).$$

Since $E_p(\mu) > 0$ for $\mu > 1$, a necessary condition for the reliable decoding of a single point is $\mu > 1$, thereby relating the size of the fundamental Voronoi region (and ultimately how many points one can transmit reliably) to the noise power, aligning well with our intuition about Gaussian channels.

- A sequence of n -dimensional lattices $\Lambda^{(n)}$ is said to be *Rogers good* (48) if

$$\lim_{n \rightarrow \infty} \frac{r_{cov}^{(n)}}{r_{eff}^{(n)}} = 1,$$

where the covering radius $r_{cov}^{(n)}$ is the radius of the smallest sphere which contains the fundamental Voronoi region of $\Lambda^{(n)}$, and the effective radius $r_{eff}^{(n)}$ is the radius of a sphere of the same volume as the fundamental Voronoi region of $\Lambda^{(n)}$.

- A sequence of n -dimensional lattices $\Lambda^{(n)}$ is said to be *good for mean-squared error quantization* if

$$\lim_{n \rightarrow \infty} G(\Lambda^{(n)}) = \frac{1}{2\pi e};$$

It may be shown that if a sequence of lattices is Rogers good, that it is also good for mean-squared error quantization (49). Furthermore, for a Rogers' good lattice Λ , it may be shown that $\sigma^2(\Lambda)$ and $V = \text{Vol}(\mathcal{V})$ are in one-to-one correspondence (up to a constant) as in (4, Appendix A); hence for a Rogers good lattice we may define either its second moment per dimension or its volume. This will be used in generating nested lattice chains.

- For any $\mathbf{s} \in \mathbb{R}^n$,

$$(\alpha(\mathbf{s} \bmod \Lambda)) \bmod \Lambda = (\alpha\mathbf{s}) \bmod \Lambda, \quad \alpha \in \mathbb{Z}. \quad (3.1)$$

$$\beta(\mathbf{s} \bmod \Lambda) = (\beta\mathbf{s}) \bmod \beta\Lambda, \quad \beta \in \mathbb{R}. \quad (3.2)$$

Finally, we include a statement of the useful “Crypto lemma” for completeness.

Lemma 1 *Crypto lemma (25; 50). For any random variable \mathbf{x} distributed over the fundamental region \mathcal{V} and statistically independent of \mathbf{U} , which is uniformly distributed over \mathcal{V} , $(\mathbf{x} + \mathbf{U}) \bmod \Lambda$ is independent of \mathbf{x} and uniformly distributed over \mathcal{V} .*

3.2 Nested lattice codes

Consider two lattices Λ and Λ_c such that $\Lambda \subseteq \Lambda_c$ with fundamental regions $\mathcal{V}, \mathcal{V}_c$ of volumes V, V_c respectively. Here Λ is termed the *coarse* lattice which is a sublattice of Λ_c , the *fine* lattice, and hence $V \geq V_c$. When transmitting over the AWGN channel, one may use the set $\mathcal{C}_{\Lambda_c, \mathcal{V}} = \{\Lambda_c \cap \mathcal{V}\}$ as the codebook. The coding rate R of this *nested* (Λ, Λ_c) *lattice pair* is defined as

$$R = \frac{1}{n} \log |\mathcal{C}_{\Lambda_c, \mathcal{V}}| = \frac{1}{n} \log \frac{V}{V_c},$$

where $\rho = |\mathcal{C}_{\Lambda_c, \mathcal{V}}|^{\frac{1}{n}} = \left(\frac{V}{V_c}\right)^{\frac{1}{n}}$ is the nesting ratio of the nested lattice pair. It was shown that there exist nested lattice pairs which achieve the capacity of the AWGN channel (25).

3.3 Nested lattice chains

In the following, we will use an extension of nested lattice codes termed nested lattice chains as in (4; 3), and shown in Figure 3 (chain of length 3). We first re-state a slightly modified version of (4, Theorem 2) on the existence of good nested lattice chains, of use in our achievability proofs.

Theorem 2 *Existence of “good” nested lattice chains (adapted from Theorem 2 of (4)). For any $P_1 \geq P_2 \geq \dots \geq P_K > 0$ and $\gamma > 0$, there exists a sequence of n -dimensional lattice $\Lambda_1 \subseteq \Lambda_2 \subseteq \dots \subseteq \Lambda_K \subseteq \Lambda_C$ ($\mathcal{V}_1 \supseteq \mathcal{V}_2 \supseteq \dots \supseteq \mathcal{V}_K \supseteq \mathcal{V}_C$) satisfying:*

- a) $\Lambda_1, \Lambda_2, \dots, \Lambda_K$ are simultaneously Rogers-good and Poltyrev-good while Λ_C is Poltyrev-good.
- b) For any $\delta > 0$, $P_i - \delta \leq \sigma^2(\Lambda_i) \leq P_i$, $1 \leq i \leq K$ for sufficiently large n .
- c) The coding rate associated with the nested lattice pair $\Lambda_K \subseteq \Lambda_C$ is $R_{K,C} = \frac{1}{n} \log \frac{V_K}{V_C} = \gamma + o_n(1)$ where $o_n(1) \rightarrow 0$ as $n \rightarrow \infty$. Moreover, for $1 \leq i < j \leq K$, the coding rate of the nested lattice pair $\Lambda_i \subseteq \Lambda_j$ is $R_{i,j} := \frac{1}{n} \log \frac{V_i}{V_j} = \frac{1}{2} \log \frac{P_i}{P_j} + o_n(1)$ and $R_{i,C} = R_{i,K} + R_{K,C} = \frac{1}{2} \log \frac{P_i}{P_K} + \gamma + o_n(1)$ ($1 \leq i \leq K-1$).

Proof: From Theorem 2 of (4) there exists a nested lattice chain which satisfies the properties a) and b) and for which $R_{K,C} = \gamma + o_n(1)$, and $R_{i,C} = \frac{1}{n} \log \frac{V_i}{V_C} = R_{K,C} + \frac{1}{2} \log \frac{P_i}{P_K} + o_n(1)$. Now notice that $R_{i,j} = \frac{1}{n} \log \frac{V_i}{V_j} = \frac{1}{n} \log \frac{V_i}{V_C} - \frac{1}{n} \log \frac{V_C}{V_j} = R_{i,C} - R_{j,C} = \frac{1}{2} \log \frac{P_i}{P_j} + o_n(1)$.

CHAPTER 4

LATTICE CODING FOR DECODE-AND-FORWARD

In this section, lattice codes are shown to achieve Decode-and-Forward performance in relay networks. To demonstrate a lattice Decode-and-Forward strategy, we introduce a lattice list decoding technique which enables the decoder to decode a list of possible codewords rather a single one. In relay channels, there are multiple links between source and destinations through multiple relays. The decoder decodes a list of codewords for each link and intersect them to obtain the single one. This strategy is shown in both single-relay and multiple-relay cases, and further combined with linearity of lattice codes in several presented multi-source scenarios.

4.1 Lattice list decoding

List decoding here refers to a decoding procedure in which, instead of outputting a single codeword corresponding to a single message, the decoder outputs a list of possible codewords which includes the correct (transmitted) one with high probability. Such a decoding scheme is useful in cooperative scenarios when a message is transmitted above the capacity of a given link (and hence the decoder would not be able to correctly distinguish the true transmitted codeword from that given link), and is combined with additional information at the receiver to decode a single message point from within the list. We present our key theorem next which bounds the list size for a lattice list decoder which will decode a list which contains the correct message with high probability.

Theorem 3 *Lattice list decoding in mixed noise. Consider the channel $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$, subject to input power constraint $\frac{1}{n}E[\mathbf{X}^T\mathbf{X}] \leq P$, where $\mathbf{Z} = \mathbf{Z}_G + \sum_{i=1}^L \mathbf{Z}_i$ is noise which is a mixture of Gaussian noise $\mathbf{Z}_G \sim \mathcal{N}(\mathbf{0}, \sigma_G^2 \mathbf{I})$ and independent noises \mathbf{Z}_i which are uniformly distributed over fundamental Voronoi regions of Rogers-good lattices with second moments P_i . Thus, \mathbf{Z} is of equivalent total variance $N = \frac{1}{n}E(\mathbf{Z}^T\mathbf{Z}) = \sigma_G^2 + \sum_{i=1}^L P_i$. For any $|L| > 2^{n(R-C(P/N))}$, $\delta > 0$, $R > C(P/N)$, and n large enough, there exists a chain of nested lattices such that the lattice list decoder can produce a list of size $|L|$, which does not contain the correct codeword with probability smaller than δ .*

Proof: Encoding: We consider a good nested lattice chain $\Lambda \subseteq \Lambda_s \subseteq \Lambda_c$ as in Figure 3 and Theorem 2, in which Λ and Λ_s are both Rogers good and Poltyrev good while Λ_c is Poltyrev good. We define the coding rate $R = \frac{1}{n} \log \frac{V}{V_c}$ and the nesting rate $R_1 = \frac{1}{2} \log \frac{V}{V_s}$. Each message $w \in \{1, \dots, 2^{nR}\}$ is one-to-one mapped to the lattice point $\mathbf{t}(w) \in \mathcal{C}_{\Lambda_c, \mathcal{V}} = \{\Lambda_c \cap \mathcal{V}\}$, and the transmitter sends $\mathbf{X} = (\mathbf{t}(w) - \mathbf{U}) \bmod \Lambda$, where \mathbf{U} is an n -dimensional dither signal (known to the encoder and decoder) uniformly distributed over \mathcal{V} .

Decoding: Upon receiving \mathbf{Y} , the receiver computes

$$\begin{aligned}
 \mathbf{Y}' &= (\alpha \mathbf{Y} + \mathbf{U}) \bmod \Lambda \\
 &= (\mathbf{t}(w) - (1 - \alpha)\mathbf{X} + \alpha\mathbf{Z}) \bmod \Lambda \\
 &= (\mathbf{t}(w) + (-(1 - \alpha)\mathbf{X} + \alpha\mathbf{Z}) \bmod \Lambda) \bmod \Lambda \\
 &= (\mathbf{t}(w) + \mathbf{Z}') \bmod \Lambda,
 \end{aligned} \tag{4.1}$$

for $\alpha \in \mathbb{R}$. We choose α to be the MMSE coefficient $\alpha = \frac{P}{P+N}$ and note that the equivalent noise $\mathbf{Z}' = (-(1-\alpha)\mathbf{X} + \alpha\mathbf{Z}) \bmod \Lambda$ is independent of $\mathbf{t}(w)$. The receiver decodes the *list* of messages

$$L_{S-D}^w(\mathbf{Y}) := \{w \mid \mathbf{t}(w) \in S_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda\}, \quad (4.2)$$

where

$$S_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') := \bigcup_{\lambda_c \in \Lambda_c} \{\lambda_c \mid \lambda_c \in (\mathbf{Y}' + \mathcal{V}_s)\},$$

is the set of lattice points $\lambda_c \in \Lambda_c$ inside \mathcal{V}_s centered at the point \mathbf{Y}' as shown in Figure 4.

Remark 1 *The notation used for the list of messages, i.e. $L_{S-D}^w(\mathbf{Y})$ should be understood as follows: the $S - D$ subscript is meant to denote the transmitter S and the receiver D , the dependence on \mathbf{Y} (rather than \mathbf{Y}') is included, though in all cases we will make the analogous transformation from \mathbf{Y} to \mathbf{Y}' as in (Equation 4.1) (but for brevity do not include this in future schemes), and the superscript w is used to recall what messages are in the list, useful in multi-source and Block Markov schemes.*

Probability of error for list decoding: Pick $\delta > 0$. In decoding a list, we require that the correct, transmitted codeword $\mathbf{t}(w)$ lies in the list with high probability as $n \rightarrow \infty$, i.e. the probability of error is (for n the blocklength or dimension of the lattices) $P_{n,e} := \Pr\{w \notin L_{S-D}^w(\mathbf{Y}) \mid w \text{ sent}\}$, which should be made less than δ as $n \rightarrow \infty$. This is easy to do with large list sizes; we bound the list size next. The following Lemma allows us to more easily bound the probability of list decoding error.

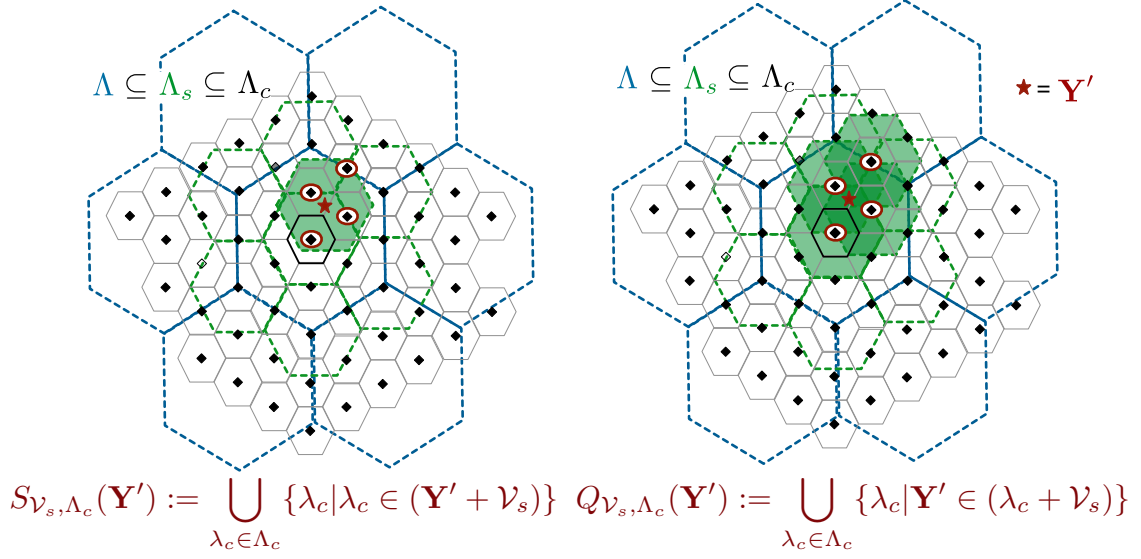


Figure 4. The two equivalent lists, in this example consisting of the four points encircled in red. The correct message lattice point is the center. Color is useful.

Lemma 4 *Equivalent decoding list. For the nested lattices $\Lambda_s \subseteq \Lambda_c$ and given $\mathbf{Y}' \in \mathbb{R}^n$, define*

$$Q_{V_s, \Lambda_c}(\mathbf{Y}') := \bigcup_{\lambda_c \in \Lambda_c} \{\lambda_c | \mathbf{Y}' \in (\lambda_c + \mathcal{V}_s)\}. \quad (4.3)$$

and

$$S_{V_s, \Lambda_c}(\mathbf{Y}') := \bigcup_{\lambda_c \in \Lambda_c} \{\lambda_c | \lambda_c \in (\mathbf{Y}' + \mathcal{V}_s)\},$$

Then the sets $S_{V_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda$ and $Q_{V_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda$ are equal.

Proof: $Q_{V_s, \Lambda_c}(\mathbf{Y}')$ is the set of $\lambda_c \in \Lambda_c$ points satisfying $\mathbf{Y}' \in (\lambda_c + \mathcal{V}_s)$. Also note that the fundamental Voronoi region \mathcal{V} of any lattice Λ is centro-symmetric ($\forall x \in \mathcal{V}$, we have that

$-x \in \mathcal{V}$) by definition of a lattice and fundamental Voronoi region (alternatively, see (51)).

Hence, for any two points x and x' , and a centro-symmetric region \mathcal{V} , $x' \in x + \mathcal{V} \Leftrightarrow x \in x' + \mathcal{V}$.

Applying this to $S_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}')$ and $Q_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}')$ yields the lemma.

We continue with the proof of Theorem 3. We first use Lemma 4 to see that the lists $S_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda$ and $Q_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda$ are equal. Next notice that the probability of error may be bounded as follows:

$$P_{n,e} = \Pr\{w \notin L_{S-D}^w(\mathbf{Y}) \mid w \text{ sent}\} \quad (4.4)$$

$$= \Pr\{\mathbf{t}(w) \notin S_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda \mid w \text{ sent}\} \quad (4.5)$$

$$= \Pr\{\mathbf{t}(w) \notin Q_{\mathcal{V}_s, \Lambda_c}(\mathbf{Y}') \bmod \Lambda \mid w \text{ sent}\} \quad (4.6)$$

$$= \Pr\{\mathbf{Y}' \notin (\mathbf{t}(w) + \mathcal{V}_s) \mid w \text{ sent}\} \quad (4.7)$$

$$= \Pr\{(\mathbf{t}(w) + \mathbf{Z}') \bmod \Lambda \notin (\mathbf{t}(w) + \mathcal{V}_s) \mid w \text{ sent}\} \quad (4.8)$$

$$= \Pr\{\mathbf{Z}' \notin \mathcal{V}_s \mid w \text{ sent}\} \quad (4.9)$$

$$\leq \Pr\{\mathbf{Z}'' \notin \mathcal{V}_s \mid w \text{ sent}\} \quad (4.10)$$

where $\mathbf{Z}' = -(1 - \alpha)\mathbf{X} + \alpha\mathbf{Z} \bmod \Lambda$ and $\mathbf{Z}'' = -(1 - \alpha)\mathbf{X} + \alpha\mathbf{Z}$. We now use Lemma 5 to show that the pdf of \mathbf{Z}'' can be upper bounded by the pdf of a Gaussian random vector of not much larger variance, which in turn is used to bound the above probability of error.

Lemma 5 *Let $\mathbf{Z}_G \sim \mathcal{N}(\mathbf{0}, \sigma_G^2 \mathbf{I})$, \mathbf{X} be uniform over the fundamental Voronoi region of the Rogers good Λ , of effective and covering radii r_{eff} and r_{cov} and second moment P , and \mathbf{Z}_i be*

uniform over the fundamental Voronoi region of the Rogers good Λ_i of effective and covering radii $r_{eff,i}$ and $r_{cov,i}$ and second moments P_i , $i = 1, \dots, L$. Let $\mathbf{Z}'' := -(1 - \alpha)\mathbf{X} + \alpha\mathbf{Z}_G + \alpha \sum_{i=1}^L \mathbf{Z}_i$. Then there exists an i.i.d. Gaussian vector

$$\mathbf{Z}^* = -(1 - \alpha)\mathbf{Z}_X^* + \alpha\mathbf{Z}_G + \alpha \sum_{i=1}^L \mathbf{Z}_i^*$$

with variance σ^2 satisfying

$$\sigma^2 \leq (1 - \alpha)^2 \left(\frac{r_{cov}}{r_{eff}} \right)^2 P + \alpha^2 \sigma_G^2 + \alpha^2 \sum_{i=1}^L \left(\frac{r_{cov,i}}{r_{eff,i}} \right)^2 P_i$$

such that the density of \mathbf{Z}'' is upper bounded as:

$$f_{\mathbf{Z}''}(\mathbf{z}) \leq e^{(c(n) + \sum_{i=1}^L c_i(n))n} f_{\mathbf{Z}^*}(\mathbf{z}) \quad (4.11)$$

where $c(n) = \ln \left(\frac{r_{cov}}{r_{eff}} \right) + \frac{1}{2} \ln 2\pi e G_{\mathcal{B}}^{(n)} + \frac{1}{n}$ and $c_i(n) = \ln \left(\frac{r_{cov,i}}{r_{eff,i}} \right) + \frac{1}{2} \ln 2\pi e G_{\mathcal{B}}^{(n)} + \frac{1}{n}$, and $G_{\mathcal{B}}^{(n)}$ is the normalized second moment of an n -dimensional ball.

Proof: The proof follows (1, Appendix A) and (25, Lemma 6 and 11) almost exactly, where the central difference with (1, Appendix A) is that we need to bound the pdf of a sum of random variables uniformly distributed over *different* Rogers good lattices rather than identical ones. This leads to the summation in the exponent of (Equation 4.11) but note that we will still have $c(n), c_i(n) \rightarrow 0$ as $n \rightarrow \infty$.

Continuing the proof of Theorem 3, according to Lemma 5,

$$P_{n,e} \leq \Pr\{\mathbf{Z}'' \notin \mathcal{V}_s\} \leq e^{(c(n) + \sum_{i=1}^L c_i(n))n} \Pr\{\mathbf{Z}^\star \notin \mathcal{V}_s\}. \quad (4.12)$$

To bound $\Pr\{\mathbf{Z}^\star \notin \mathcal{V}_s\}$, we first need to show that the VNR of Λ_s relative to \mathbf{Z}^\star , μ , is greater than one:

$$\mu = \frac{(V(\Lambda_s))^{2/n}}{2\pi e \sigma^2} + o_n(1) \geq \frac{(V(\Lambda))^{2/n} / 2^{2R_1}}{2\pi e \frac{PN}{P+N}} + o_n(1) \quad (4.13)$$

$$= \frac{1}{2^{2R_1}} \frac{1}{2\pi e G(\Lambda)} \frac{P}{\frac{PN}{P+N}} + o_n(1) \quad (4.14)$$

$$= \frac{1}{2^{2R_1}} \left(1 + \frac{P}{N}\right) + o_n(1) \quad (4.15)$$

$$= 2^{2(C(P/N) - R_1)} + o_n(1) \quad (4.16)$$

where (Equation 6.12) follows from Lemma 5, the fact that Λ and Λ_i ($1 \leq i \leq L$) are all Rogers good, and recalling that $\alpha = \frac{P}{P+N}$, where $N = \sigma_G^2 + \sum_{i=1}^L P_i$. Then (Equation 6.13) follows from the definition of $G(\Lambda)$ and (Equation 4.15) follows as Λ is Rogers good. Combining (Equation 4.12), (Equation 6.14), and the fact that Λ_s is Poltyrev good, by definition

$$P_{n,e} \leq e^{(c(n) + \sum_{i=1}^L c_i(n))n} \Pr\{\mathbf{Z}^\star \notin \mathcal{V}_s\} \quad (4.17)$$

$$\leq e^{(c(n) + \sum_{i=1}^L c_i(n))n} e^{-n(E_p(\mu) - o_n(1))} \quad (4.18)$$

$$\leq e^{-n(E_p(2^{2(C(P/N) - R_1)}) - o_n(1))} \quad (4.19)$$

where (Equation 4.19) follows as $\Lambda, \Lambda_1, \dots, \Lambda_L$ are Rogers good and hence $c(n), c_i(n)$ all tend to 0 as $n \rightarrow \infty$.

To ensure $P_{n,e} < \delta$ as $n \rightarrow \infty$ we need $C(P/N) - R_1 > 0$, where $R_1 = \frac{1}{n} \log(\frac{V}{V_s}) = \frac{1}{2} \log(\frac{P}{P_s}) + o_n(1)$, and n sufficiently large. By choosing an appropriate P_s according to Theorem 2, we may set $R_1 = \frac{1}{n} \log(\frac{V}{V_s}) = C(P/N) - \epsilon_n$ for any $\epsilon_n > 0$. Combining these, we obtain

$$V_s = \left(\frac{N}{P+N} \right)^{n/2} 2^{n\epsilon_n} V. \quad (4.20)$$

The cardinality of the decoded list $L_{S-D}^w(\mathbf{Y})$, in which the true codeword lies with high probability as $n \rightarrow \infty$, may be bounded as

$$|L_{S-D}^w(\mathbf{Y})| = \frac{V_s}{V_c} = \frac{\frac{N^{n/2}V}{(P+N)^{n/2}} 2^{n\epsilon_n}}{\frac{V}{2^{nR}}} = 2^{n(R-C(P/N))} 2^{n\epsilon_n},$$

since $R = \frac{1}{n} \log(\frac{V}{V_c})$. Setting $\epsilon_n = \frac{1}{n^2}$, $2^{n\epsilon_n} \rightarrow 1$, and so $|L_{S-D}^w(\mathbf{Y})| \rightarrow 2^{n(R-C(P/N))}$ as $n \rightarrow \infty$.

Remark 2 Note that in our Theorem statement we have assumed $R > C(P/N)$; when $R < C(P/N)$, the decoder can decode an unique codeword with high probability, as stated in Lemma 6.

Lemma 6 *Lattice unique decoding in mixed noise. Consider the channel $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$, subject to input power constraint $\frac{1}{n} E[\mathbf{X}^T \mathbf{X}] \leq P$, where $\mathbf{Z} = \mathbf{Z}_G + \sum_{i=1}^L \mathbf{Z}_i$ is noise which is a mixture of Gaussian noise $\mathbf{Z}_G \sim \mathcal{N}(\mathbf{0}, \sigma_G^2 \mathbf{I})$ and independent noises \mathbf{Z}_i which are uniformly distributed over fundamental Voronoi regions of Rogers-good lattices with second moments P_i . Thus, \mathbf{Z} is*

of equivalent variance $N = \frac{1}{n}\mathbb{E}(\mathbf{Z}^T\mathbf{Z}) = \sigma_G^2 + \sum_{i=1}^L P_i$. For any $\delta > 0$, $R < C(P/N)$, and n large enough, there exist lattice codebooks such that the decoder can decode a unique codeword with probability of error smaller than δ . **Proof:** This lemma can be derived as a special case of Compute-and-Forward (1, Theorem 1); in particular this is found in (1, Example 2), where the decoder is interested in one of the messages and treats all other messages as noise. We may view \mathbf{Z}_i in this lemma as the signals from other (lattice-codeword based) transmitters in (1, Example 2).

4.2 Decode-and-Forward for the AWGN single relay channel

We first show that nested lattice codes may be used to achieve the Decode-and-Forward (DF) rate of (8, Theorem 5) for the Gaussian relay channel using nested lattice codes at the source and relay, and a lattice list decoder at the destination. We then extend this result to show that the generalized DF rate for a Gaussian relay network with a single source, a single destination and multiple DF relays may also be achieved using an extension of the single relay lattice-based achievability scheme.

Consider a relay channel in which the source node S , with channel input X_S transmits a message $w \in \{1, 2, \dots, 2^{nR}\}$ to destination node D which has access to the channel output Y_D and is aided by a relay node R with channel input and output X_R and Y_R . Input and output random variables lie in \mathbb{R} . At each channel use, the channel inputs and outputs are related as $Y_D = X_S + X_R + Z_D$, $Y_R = X_S + Z_R$, where Z_R, Z_D are independent Gaussian random variables of zero mean and variance N_R and N_D respectively. Let \mathbf{X}_S denote a sequence of n

channel inputs (a row vector), and similarly, let $\mathbf{X}_R, \mathbf{Y}_R, \mathbf{Y}_D$ all denote the length n sequences of channel inputs and outputs. Then the channel may be described by

$$\mathbf{Y}_D = \mathbf{X}_S + \mathbf{X}_R + \mathbf{Z}_D, \quad \mathbf{Y}_R = \mathbf{X}_S + \mathbf{Z}_R, \quad (4.21)$$

where $\mathbf{Z}_D \sim \mathcal{N}(\mathbf{0}, N_D \mathbf{I})$ and $\mathbf{Z}_R \sim \mathcal{N}(\mathbf{0}, N_R \mathbf{I})$, and inputs are subject to the power constraints $\frac{1}{n} E[\mathbf{X}_S^T \mathbf{X}_S] \leq P$ and $\frac{1}{n} E[\mathbf{X}_R^T \mathbf{X}_R] \leq P_R$.

An $(2^{nR}, n)$ code for the relay channel consists of the set of messages w uniformly distributed over $\mathcal{M} := \{1, 2, \dots, 2^{nR}\}$, an encoding function $X_S^n : \mathcal{M} \rightarrow \mathbb{R}^n$ satisfying the power constraint, a set of relay functions $\{f_i\}_{i=1}^n$ such that the relay channel input at time i is a function of the previously received relay channel outputs from channel uses 1 to $i-1$, $X_{R,i} = f_i(Y_{R,1}, \dots, Y_{R,i-1})$, and finally a decoding function $g : \mathcal{Y}_D^n \rightarrow \mathcal{M}$ which yields the message estimate $\hat{w} := g(\mathbf{Y}_D^n)$. We define the average probability of error of the code to be $P_{n,e} := \frac{1}{2^{nR}} \sum_{w \in \mathcal{M}} \Pr\{\hat{w} \neq w | w \text{ sent}\}$. The rate R is then said to be achievable by a relay channel if, for any $\epsilon > 0$ and for sufficiently large n , there exists an $(2^{nR}, n)$ code such that $P_{n,e} < \epsilon$. The capacity C of the relay channel is the supremum of the set of achievable rates.

We are first interested in showing that the DF rate achieved by Gaussian random codebooks of (8, Theorem 5) may be achieved using lattice codes. As outlined in (10), this DF rate may be achieved using irregular encoding / successive decoding as in (8), regular encoding / sliding-window decoding as first shown in (52), and using regular encoding / backwards decoding as in (53).

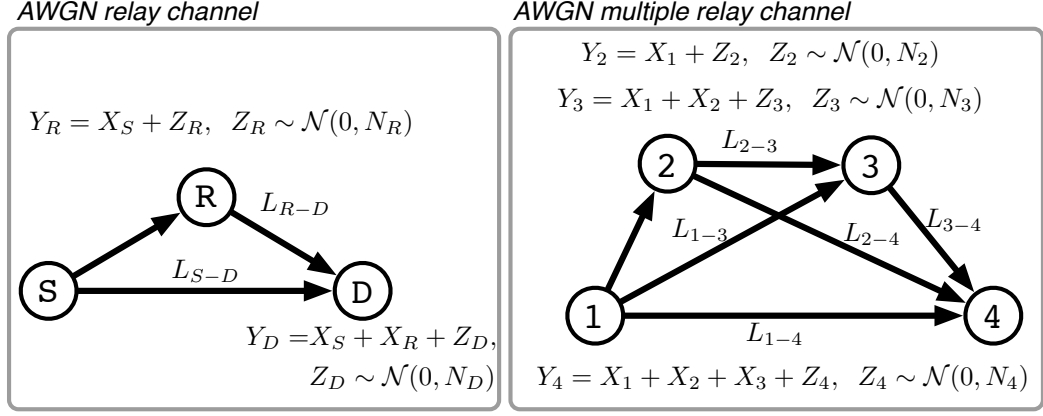


Figure 5. The two Gaussian relay channels under consideration in Section 4.2 and Section 4.4.

For the AWGN relay channel we have assumed a particular relay order (2,3) for our achievability scheme and shown the equivalent channel model used in deriving the achievable rate rather than the general channel model.

We will mimic the regular encoding/sliding-window decoding scheme of (12), which includes: (1) random coding, (2) list decoding, (3) two joint typicality decoding steps, (4) coding for the cooperative multiple-access channel, (5) superposition coding and (6) block Markov encoding. We re-derive the DF rate, following the achievability scheme of (12), but with lattice codes replacing the random Gaussian coding techniques. Of particular importance is the usage of two lattice list decoders to replace two joint typicality decoding steps in the random coding achievability scheme.

	Block 1	Block 2	Block 3	Block 4
Encoding:				
\textcircled{S}	$X'_1(w_1) + X'_2(1)$	$X'_1(w_2) + X'_2(w_1)$	$X'_1(w_3) + X'_2(w_2)$	$X'_1(1) + X'_2(w_3)$
\textcircled{R}	$X'_2(1)$	$X'_2(w_1)$	$X'_2(w_2)$	$X'_2(w_3)$
Decoding:				
\textcircled{R}	w_1	w_2	w_3	w_4
\textcircled{D}	$L_{S-D}^{w_1}$	$L_{R-D}^{w_1}$ $L_{S-D}^{w_2}$	$L_{R-D}^{w_2}$ $L_{S-D}^{w_3}$	$L_{R-D}^{w_3}$

Figure 6. Lattice Decode-and-Forward scheme for the AWGN relay channel.

Theorem 7 *Lattices achieve the DF rate achieved by random Gaussian codebooks for the relay channel. The following Decode-and-Forward rates can be achieved using nested lattice codes for the Gaussian relay channel described by (Equation 4.21):*

$$R < \max_{\alpha \in [0,1]} \min \left\{ \frac{1}{2} \log \left(1 + \frac{\alpha P}{N_R} \right), \frac{1}{2} \log \left(1 + \frac{P + P_R + 2\sqrt{\bar{\alpha} P P_R}}{N_D} \right) \right\}, \quad \bar{\alpha} = 1 - \alpha. \quad (4.22)$$

Proof:

Codebook construction: We consider two nested lattice chains of length three $\Lambda_1 \subseteq \Lambda_{s1} \subseteq \Lambda_{c1}$, and $\Lambda_2 \subseteq \Lambda_{s2} \subseteq \Lambda_{c2}$ whose existence is guaranteed by Theorem 2, and whose parameters P_i, γ we still need to specify. The nested lattice pairs $(\Lambda_1, \Lambda_{c1})$ and $(\Lambda_2, \Lambda_{c2})$ are used to construct lattice codebooks of coding rate R with $\sigma^2(\Lambda_1) = \alpha P$ and $\sigma^2(\Lambda_2) = \bar{\alpha} P$ for given $\alpha \in [0, 1]$. Since Λ_1 and Λ_2 will not be the finest lattice in the chain, they will be Rogers

good, and hence $\sigma^2(\Lambda_1) = \alpha P$ will define the volume of Λ_1, V_1 , and $\sigma^2(\Lambda_2) = \bar{\alpha} P$ will define the volume of Λ_2, V_2 . Since $(\Lambda_1, \Lambda_{c1})$ and $(\Lambda_2, \Lambda_{c2})$ are used to construct lattice codebooks of coding rate

$$R = \frac{1}{n} \log \left(\frac{V_1}{V_{c1}} \right) = \frac{1}{n} \log \left(\frac{V_2}{V_{c2}} \right),$$

this will in turn define V_{c1} in terms of V_1 and rate R ; similarly for V_{c2} in terms of V_2 and rate R . Since Λ_{c1} and Λ_{c2} are only Poltyrev good, we may obtain the needed V_{c1}, V_{c2} by appropriate selection of γ in Theorem 2. Finally, the lattices Λ_{s1} and Λ_{s2} (whose second moments we may still specify arbitrarily, and which will be used for lattice list decoding at the destination node) will also be Rogers good and their volumes, or equivalently, second moments, will be selected in the course of the proof.

Randomly map the messages $w \in \{1, 2, \dots, 2^{nR}\}$ to codewords $\mathbf{t}_1(w) \in \mathcal{C}_1 = \{\Lambda_{c1} \cap \mathcal{V}_1\}$ and $\mathbf{t}_2(w) \in \mathcal{C}_2 = \{\Lambda_{c2} \cap \mathcal{V}_2\}$. Let these two mappings be independent and known to all nodes.

We use block Markov coding and define w_b as the new message index to be sent in block b ($b = 1, 2, \dots, B$); define $w_0 = 1$. At the end of block $b-1$, the receiver knows (w_1, \dots, w_{b-2}) and the relay knows (w_1, \dots, w_{b-1}) . We let $\mathbf{Y}_R(b), \mathbf{Y}_D(b)$ denote the vectors of length n of received signals at the relay and the destination, respectively, during the b -th block, and $\mathbf{U}_1(b), \mathbf{U}_2(b)$ denote dithers during block b known to all nodes which are i.i.d., change from block to block, and are uniformly distributed over \mathcal{V}_1 and \mathcal{V}_2 respectively. The encoding and decoding steps are outlined in Figure 6.

Encoding: During the b -th block, the transmitter sends the superposition (sum) $\mathbf{X}_S(w_b, w_{b-1}) = \mathbf{X}'_1(w_b) + \mathbf{X}'_2(w_{b-1})$, and the relay sends $\mathbf{X}_R(w_{b-1})$, where

$$\begin{aligned}\mathbf{X}'_1(w_b) &= (\mathbf{t}_1(w_b) - \mathbf{U}_1(b)) \mod \Lambda_1, \\ \mathbf{X}'_2(w_{b-1}) &= (\mathbf{t}_2(w_{b-1}) - \mathbf{U}_2(b-1)) \mod \Lambda_2 \\ \mathbf{X}_R(w_{b-1}) &= \sqrt{\frac{P_R}{\alpha P}} \mathbf{X}'_2(w_{b-1}) = \left(\sqrt{\frac{P_R}{\alpha P}} \mathbf{t}_2(w_{b-1}) - \sqrt{\frac{P_R}{\alpha P}} \mathbf{U}_2(b-1) \right) \mod \sqrt{\frac{P_R}{\alpha P}} \Lambda_2.\end{aligned}$$

By the Crypto lemma $\mathbf{X}'_1(w_b)$ and $\mathbf{X}'_2(w_{b-1})$ are uniformly distributed over \mathcal{V}_1 and \mathcal{V}_2 and independent of all else.

Decoding:

1. At the b -th block, the relay knows w_{b-1} and consequently $\mathbf{X}'_2(w_{b-1})$, and so may decode the message w_b from the received signal $\mathbf{Y}_R(b) - \mathbf{X}'_2(w_{b-1}) = \mathbf{X}'_1(w_b) + \mathbf{Z}_R(b)$ as long as $R < C(\alpha P/N_R)$, since $(\Lambda_1, \Lambda_{c1})$ may achieve the capacity of the point-to-point channel (25) or Lemma 6.

2. The receiver first decodes a list of messages w_{b-1} , $L_{R-D}^{w_{b-1}}(\mathbf{Y}_D(b))$, defined according to (Equation 4.2) as

$$L_{R-D}^{w_{b-1}}(\mathbf{Y}_D(b)) = \{w_{b-1} \mid \mathbf{t}_2(w_{b-1}) \in S_{\kappa \mathcal{V}_{s2}, \kappa \Lambda_{c2}}(\mathbf{Y}'_D(b)) \mod \kappa \Lambda_2\}, \quad (4.23)$$

of asymptotic size $2^{n(R-R_R)}$ from the signal

$$\mathbf{Y}_D(b) = \mathbf{X}_S(w_b, w_{b-1}) + \mathbf{X}_R(w_{b-1}) + \mathbf{Z}_D(b) \quad (4.24)$$

$$= \mathbf{X}'_1(w_b) + \kappa \mathbf{X}'_2(w_{b-1}) + \mathbf{Z}_D(b) \quad (4.25)$$

for $\kappa = \left(1 + \sqrt{\frac{P_R}{\alpha P}}\right)$ using the lattice list decoding scheme of Theorem 3. Notice that Theorem 3 is applicable as the “noise” in decoding a list of w_{b-1} from $\mathbf{Y}_D(b)$ is composed of the sum of a Gaussian signal $\mathbf{Z}_D(b)$ and $\mathbf{X}'_1(w_b)$ which is uniformly distributed over the fundamental Voronoi region of the Rogers good lattice of second moment αP . The equivalent noise variance in Theorem 3 is thus $\alpha P + N_D$, and the capacity of the channel is (25) $C(\kappa^2 \bar{\alpha} P / (\alpha P + N_D)) = C((\sqrt{\alpha P} + \sqrt{P_R})^2 / (\alpha P + N_D))$. We may thus obtain a list of size $2^{n(R-R_R)}$ as long as

$$R_R < \frac{1}{2} \log \left(\frac{\kappa^2 \bar{\alpha} P}{\frac{\kappa^2 \bar{\alpha} P (\alpha P + N_D)}{\kappa^2 \bar{\alpha} P + \alpha P + N_D}} \right) = \frac{1}{2} \log \left(1 + \frac{(\sqrt{\alpha P} + \sqrt{P_R})^2}{\alpha P + N_D} \right). \quad (4.26)$$

One may directly apply Theorem 3; for additional details on this step, please see Appendix .1.

3. A second list of messages w_{b-1} was obtained at the end of block $b-1$ from the direct link between the transmitter node S and the destination node D, denoted as $L_{S-D}^{w_{b-1}}(\mathbf{Y}_D(b-1) - \kappa \mathbf{X}'_2(w_{b-2}))$ defined according to (Equation 4.2) and analogous to (Equation 4.23) using a lattice list decoder. We now describe the formation of the list $L_{S-D}^{w_b}(\mathbf{Y}_D(b) - \kappa \mathbf{X}'_2(w_{b-1}))$ in block b which will be used in block $b+1$. Assuming that the receiver has decoded w_{b-1} successfully, it subtracts $\kappa \mathbf{X}'_2(w_{b-1})$ from $\mathbf{Y}_D(b)$: $\mathbf{Y}_D(b) - \kappa \mathbf{X}'_2(w_{b-1}) = \mathbf{X}'_1(w_b) + \mathbf{Z}_D(b)$, and then decodes another list of possible messages w_b of asymptotic size $2^{n(R-C(\alpha P/(N_D)))}$ using

Theorem 3. This is done using the nested lattice chain $\Lambda_1 \subseteq \Lambda_{s1} \subseteq \Lambda_{c1}$. Again, Theorem 3 is applicable as we have a channel $\mathbf{X}'_1(w_b) + \mathbf{Z}_D(b)$ of capacity $C(P/N_D)$ where the noise is purely Gaussian of second moment N_D . Here, choose the list decoding lattice Λ_{s1} to have a fundamental Voronoi region of volume approaching $V_{s1} = \left(\frac{N_D}{\alpha P + N_D}\right)^{n/2} V_1$ asymptotically (analogous to (Equation 4.20)) so that the size of the decoded list approaches $2^{n(R-C(\alpha P/(N_D)))}$. Notice that this choice of $V_{s1} < V_1$ and hence is permissible by Theorem 2 (as $P_1 > P_{s1}$). For the interesting case when R approaches $\frac{1}{2} \log \left(1 + \frac{P+P_R+2\sqrt{\alpha P P_R}}{N_D}\right)$ (and hence list decoding is needed / relevant), $V_{c1} = \left(\frac{N_D}{P+P_R+2\sqrt{\alpha P P_R}+N_D}\right)^{n/2} V_1$ asymptotically in the sense of (Equation 4.20). Thus $V_{c1} < V_{s1} < V_1$ as needed.

4. The receiver now decodes w_{b-1} by intersecting two independent lists $L_{R-D}^{w_{b-1}}(\mathbf{Y}_D(b))$ and $L_{S-D}^{w_{b-1}}(\mathbf{Y}_D(b-1) - \kappa \mathbf{X}'_2(w_{b-2}))$ and declares a success if there is a unique w_{b-1} in this intersection. Errors are declared if there is no, or multiple messages in this intersection. We are guaranteed by Theorem 3 that the correct message will lie in each list, and hence also in their intersection, with high probability by appropriate choice V_{s1} and V_{s2} . To see that no more than one message will lie in the list, notice that the two lists are *independent* due to the random and independent mappings between the message and two codeword sets. Thus, following the arguments surrounding (8, Eq. (27) and Lemma 3), or alternatively by independence of the lists and applying (54, Packing Lemma), with high probability, there is no more than one correct message in this intersection if $R - C(\alpha P/(N_2)) - R_R < 0$, or

$$R < \frac{1}{2} \log \left(1 + \frac{\alpha P}{N_D}\right) + R_R < \frac{1}{2} \log \left(1 + \frac{P + P_R + 2\sqrt{\alpha P P_R}}{N_D}\right).$$

Remark 3 *While we have mimicked the regular encoding / sliding window decoding method to achieve the DF rate, lattice list decoding may equally be used in the irregular encoding and backwards decoding schemes. The intuition we want to reinforce is that one may obtain similar results to random-coding based DF schemes using lattice codes by intersecting multiple independent lists to decode a unique message. Furthermore, as the lattice list decoder is a Euclidean lattice decoder, it does not increase the complexity at the decoder. We note that using lists is not necessary – other novel lattice-based schemes can be used instead of lattice list decoding such as (6) to achieve the same DF rate region.*

4.3 Decode-and-Forward for the AWGN multi-relay channel

We now show that nested lattice codes may also be used to achieve the DF rates of the single source, single destination multi-level relay channel (9; 12; 10). Here, all definitions remain the same as in Section 4.2; changing the channel model to account for an arbitrary number of full-duplex relays. For the 2 relay scenario we show the input/output relations used in deriving achievable rates in Figure 5. In general we would for example have $Y_2 = X_1 + X_2 + X_3 + Z_2$, but that, for our achievability scheme we assume a relay order (e.g. 2 then 3) which results in the equivalent input/output equation $Y_2 = X_1 + Z_2$ at node 2. This is equivalent due to the achievability scheme we will propose combined with the assumed relaying order, in which node 2 will be able to cancel out all signals transmitted by itself as well as node 3 (more generally, node i may cancel out all relay transmissions “further” in the relay order than itself).

The central idea remains the same – we cooperate via a series of lattice list decoders and replace multiple joint typicality checks with the intersection of multiple independent lists ob-

tained via the lattice list decoder. For clarity, we focus on the two-relay case as in Figure 5, but the results may be extended to the N -relay case in a straightforward manner. Let $\pi(\cdot)$ denote a permutation (or ordering) of the relays. In the $N = 2$ case as shown in Figure 5 we have two possible permutations: the first the identity permutation $\pi(2) = 2, \pi(3) = 3$ and the second $\pi(2) = 3, \pi(3) = 2$.

The channel model is expressed as (a node's own signal is omitted as it may subtract it off)

$$\mathbf{Y}_2 = \mathbf{X}_1 + \mathbf{X}_3 + \mathbf{Z}_2$$

$$\mathbf{Y}_3 = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}_3$$

$$\mathbf{Y}_4 = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3 + \mathbf{Z}_4,$$

where $\mathbf{Z}_2 \sim \mathcal{N}(\mathbf{0}, N_2\mathbf{I})$, $\mathbf{Z}_3 \sim \mathcal{N}(\mathbf{0}, N_3\mathbf{I})$ and $\mathbf{Z}_4 \sim \mathcal{N}(\mathbf{0}, N_4\mathbf{I})$, and nodes are subject to input power constraints $\frac{1}{n}E[\mathbf{X}_1^T\mathbf{X}_1] \leq P_1$, $\frac{1}{n}E[\mathbf{X}_2^T\mathbf{X}_2] \leq P_2$, and $\frac{1}{n}E[\mathbf{X}_3^T\mathbf{X}_3] \leq P_3$.

Theorem 8 *Lattices achieve the DF rate achieved by Gaussian random codebooks for the multi-relay channel. The following rate R is achievable using nested lattice codes for the Gaussian two relay channel described by (9):*

$$R < \max_{\pi(\cdot)} \max_{0 \leq \alpha_1, \beta_1, \alpha_2 \leq 1} \min \left\{ C \left(\frac{\alpha_1 P_1}{N_{\pi(2)}} \right), C \left(\frac{\alpha_1 P_1 + (\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_{\pi(2)}})^2}{N_{\pi(3)}} \right), \right. \\ \left. C \left(\frac{\alpha_1 P_1 + (\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_{\pi(2)}})^2 + \left(\sqrt{(1 - \alpha_1 - \beta_1 P_1)} + \sqrt{(1 - \alpha_2) P_{\pi(2)}} + \sqrt{P_{\pi(3)}} \right)^2}{N_4} \right) \right\}$$

The proof of Theorem 8 may be found in Appendix .2, and follows along the same lines as Theorem 7.

4.4 The AWGN two-way relay channel with direct links

We now illustrate how list decoding may be combined with the linearity of lattice codes in more general networks by considering two examples. In particular, we consider relay networks in which two messages are communicated, along relayed and direct links, as opposed to the single message case previously considered. The relay channel may be viewed as strictly cooperative in the sense that all nodes aid in the transmission of the same message and the only impairment is noise; the presence of multiple messages leads to the notion of interference and the possibility of decoding combinations of messages.

We again focus on demonstrating the utility of lattices in DF-based achievability schemes. In the previous section it was demonstrated that lattices may achieve *the same* rates as Gaussian random coding based schemes. Here, the presence of multiple messages/sources gives lattices a potential rate benefit over random coding-based schemes, as encoders and decoders may exploit the linearity of the lattice codes to better decode a linear combination of messages. Often, such a linear combination is sufficient to extract the desired messages if combined with the appropriate side-information, and may enlarge the achievable rate region for certain channel conditions. In this section, we demonstrate two examples of combining Compute-and-Forward based decoding of the sum of signals at relays with direct link side-information in: 1) the two-way relay channel with direct links and 2) the multiple-access relay channel. To the best of our knowledge, these are the first lattice-coding based achievable rate regions for these channels.

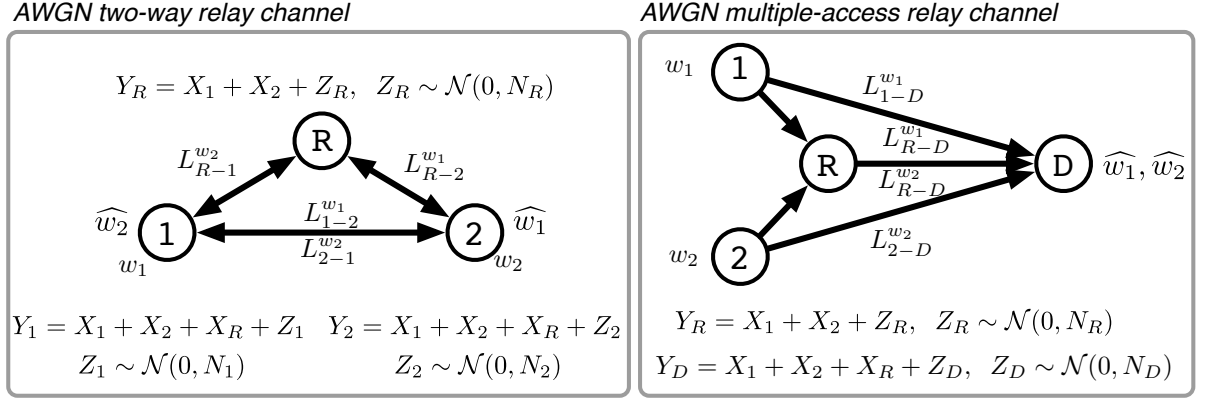


Figure 7. The AWGN two-way relay channel with direct links and the AWGN multiple-access relay channel. We illustrate the lists L_{i-j}^w of messages w carried by the codewords at node i and list decoded according to Theorem 3 at node j .

The two-way relay channel is the logical extension of the classical relay channel for one-way point-to-point communication aided by a relay to allow for two-way communication. While the capacity region is in general unknown, it is known for half-duplex channel models under the 2-phase MABC protocol (55), to within 1/2 bit for the full-duplex Gaussian channel model with no direct links (3; 2), and to within 2 bits for the same model with direct links in certain cases (56).

Random coding techniques employing DF, CF, and AF relays have been the most common in deriving achievable rate regions for the two-way relay channel, but a handful of work (57; 3; 2; 58) has considered lattice-based schemes which, in a DF-like setting, effectively exploit the additive nature of the Gaussian noise channel in allowing the sum of the two transmitted lattice points to be decoded at the relay. The intuitive gains of decoding the sum of the messages

rather than the individual messages stem from the absence of the classical multiple-access sum constraints. This sum-rate point is forwarded to the terminal which utilizes its own-message side-information to subtract off its own message from the decoded sum. While random coding schemes have been used in deriving achievable rate regions in the presence of direct links, lattice codes – of interest in order to exploit the ability to decode the sum of messages at the relay – have so far not been used. We present such a lattice-based scheme next.

The two-way Gaussian relay channel with direct links consists of two terminal nodes with inputs X_1, X_2 with power constraints P_1, P_2 (without loss of generality, it is assumed $P_1 \geq P_2$) and outputs Y_1, Y_2 which wish to exchange messages $w_1 \in \{1, 2, \dots, 2^{nR_1}\}$ and $w_2 \in \{1, 2, \dots, 2^{nR_2}\}$ with the help of the relay with input X_R of power P_R and output Y_R . We assume, without loss of generality (WLOG), the channel:

$$\mathbf{Y}_1 = \mathbf{X}_R + h_{21}\mathbf{X}_2 + \mathbf{Z}_1, \quad \mathbf{Z}_1 \sim \mathcal{N}(\mathbf{0}, N_1\mathbf{I})$$

$$\mathbf{Y}_2 = \mathbf{X}_R + h_{12}\mathbf{X}_1 + \mathbf{Z}_2, \quad \mathbf{Z}_2 \sim \mathcal{N}(\mathbf{0}, N_2\mathbf{I})$$

$$\mathbf{Y}_R = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}_R, \quad \mathbf{Z}_R \sim \mathcal{N}(\mathbf{0}, N_R\mathbf{I}),$$

subject to input power constraints $\frac{1}{n}E[\mathbf{X}_1^T\mathbf{X}_1] \leq P_1$, $\frac{1}{n}E[\mathbf{X}_2^T\mathbf{X}_2] \leq P_2$, $\frac{1}{n}E[\mathbf{X}_R^T\mathbf{X}_R] \leq P_R$ and real constants h_{12}, h_{21} . The channel model is shown in Figure 7, and all input and output alphabets are \mathbb{R} .

An $(2^{nR_1}, 2^{nR_2}, n)$ code for the two-relay channel consists of the two sets of messages w_i , $i = 1, 2$ uniformly distributed over $\mathcal{M}_i := \{1, 2, \dots, 2^{nR_i}\}$, and two encoding functions

$X_i^n : \mathcal{M}_i \rightarrow \mathbb{R}^n$ (shortened to \mathbf{X}_i) satisfying the power constraints P_i , a set of relay functions $\{f_j\}_{j=1}^n$ such that the relay channel input at time j is a function of the previously received relay channel outputs from channel uses 1 to $j-1$, $X_{R,j} = f_j(Y_{R,1}, \dots, Y_{R,j-1})$, and finally two decoding functions $g_i : \mathcal{Y}_i^n \times \mathcal{M}_i \rightarrow \mathcal{M}_{\bar{i}}$ which yields the message estimates $\hat{w}_{\bar{i}} := g_i(Y_i^n, w_i)$ for $\bar{i} = \{1, 2\} \setminus i$. We define the average probability of error of the code to be $P_{n,e} := \frac{1}{2^{n(R_1+R_2)}} \sum_{w_1 \in \mathcal{M}_1, w_2 \in \mathcal{M}_2} \Pr\{(\hat{w}_1, \hat{w}_2) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\}$. The rate pair (R_1, R_2) is then said to be achievable by the two-relay channel if, for any $\epsilon > 0$ and for sufficiently large n , there exists an $(2^{nR_1}, 2^{nR_2}, n)$ code such that $P_{n,e} < \epsilon$. The capacity region C of the two-way relay channel is the supremum of the set of achievable rate pairs.

Theorem 9 *Lattices in two-way relay channels with direct links. The following rates are achievable for the two-way AWGN relay channel with direct links*

$$R_1 \leq \min \left(\left[\frac{1}{2} \log \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{h_{12}^2 P_1 + P_R}{N_2} \right) \right) \quad (4.27)$$

$$R_2 \leq \min \left(\left[\frac{1}{2} \log \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{h_{21}^2 P_2 + P_R}{N_1} \right) \right). \quad (4.28)$$

Proof: The achievability proof combines a lattice version of regular encoding/sliding window decoding scheme (to take advantage of the direct link), decoding of the sum of transmitted signals at the relay using nested coarse lattices to take care of the asymmetric powers, as in (3), a lattice binning technique equivalent to the random binning technique developed by (59), and lattice list decoding at the terminal nodes to combine direct and relayed information.

	Block 1	Block 2	Block 3	Block 4
Encoding:				
①	$X_1(w_{11})$	$X_1(w_{12})$	$X_1(w_{13})$	$X_1(1)$
②	$X_2(w_{21})$	$X_2(w_{21})$	$X_2(w_{23})$	$X_2(1)$
③	$X_R(1)$	$X_R(T(1))$	$X_R(T(2))$	$X_R(T(3))$
Decoding:				
③	$T(1)$	$T(2)$	$T(3)$	
①	$L_{2-1}^{w_{21}}$	$L_{R-1}^{w_{21}}$ $L_{2-1}^{w_{22}}$	$L_{R-1}^{w_{22}}$ $L_{2-1}^{w_{23}}$	$L_{R-1}^{w_{23}}$
②	$L_{1-2}^{w_{11}}$	$L_{R-2}^{w_{11}}$ $L_{1-2}^{w_{12}}$	$L_{R-2}^{w_{12}}$ $L_{1-2}^{w_{13}}$	$L_{R-2}^{w_{13}}$

Figure 8. Lattice Decode-and-Forward scheme for the AWGN two-way relay channel with direct links.

Codebook construction: Assume WLOG that $P_1 > P_2$. We construct two nested lattice chains according to Theorem 2. The first consists of the lattices $\Lambda_1, \Lambda_2, \Lambda_{s1}, \Lambda_{s2}, \Lambda_{c1}, \Lambda_{c2}$ all nested such that:

- $\Lambda_1 \subseteq \Lambda_{s1} \subseteq \Lambda_{c1}$ and $\Lambda_2 \subseteq \Lambda_{s2} \subseteq \Lambda_{c2}$; the coarsest lattice is Λ_1 or Λ_2 and the finest is Λ_{c1} or Λ_{c2} .
- $\sigma^2(\Lambda_1) = P_1, \sigma^2(\Lambda_2) = P_2$
- the coding rate of $(\Lambda_1, \Lambda_{c1})$ is $R_1 = \frac{1}{n} \log \left(\frac{V_1}{V_{c1}} \right) = \frac{1}{2} \log \left(\frac{P_1}{P_{c1}} \right) + o_n(1)$, and that of $(\Lambda_2, \Lambda_{c2})$ is $R_2 = \frac{1}{n} \log \left(\frac{V_2}{V_{c2}} \right) = \frac{1}{2} \log \left(\frac{P_2}{P_{c2}} \right) + o_n(1)$. Associate each message $w_1 \in \{1, \dots, 2^{nR_1}\}$

with $\mathbf{t}_1(w_1) \in \mathcal{C}_1 = \{\Lambda_{c1} \cap \mathcal{V}_1\}$ and each message $w_2 \in \{1, \dots, 2^{nR_2}\}$ with $\mathbf{t}_2(w_2) \in \mathcal{C}_2 = \{\Lambda_{c2} \cap \mathcal{V}_2\}$.

- if $V_{c1} > V_{c2}$ (determined by relative values of R_1, P_1 and R_2, P_2 in the above), then $\Lambda_{c1} \subseteq \Lambda_{c2}$, implying Λ_{c1} may be Rogers good and hence we may guarantee the desired V_{c1} by proper selection of P_{c1} in Theorem 2 (as $R_1 = \frac{1}{2} \log \left(\frac{P_1}{P_{c1}} \right) + o_n(1) = \frac{1}{n} \log \left(\frac{V_1}{V_{c1}} \right)$); otherwise by proper selection of γ in Theorem 2 (and likewise for Λ_{c2}).
- the lattices Λ_{s1} and Λ_{s2} which will be used for lattice list decoding at node 2 and 1 respectively are both Rogers good and hence may be specified by the volumes of their fundamental Voronoi regions V_{s1} and V_{s2} (under the constraints $V_1 \geq V_{s1} \geq V_{c1}$ and $V_2 \geq V_{s2} \geq V_{c2}$), or the corresponding P_{c1}, P_{c2} . These will be chosen in the course of the proof.
- Then final relative ordering of the six lattices will then depend on the relative sizes of their fundamental region volumes.

We also construct a nested lattice chain of $\Lambda_R, \Lambda_{sR1}, \Lambda_{sR2}, \Lambda_{cR}$ according to Theorem 2 such that:

- $\Lambda_R \subseteq \Lambda_{sR1} \subseteq \Lambda_{sR2} \subseteq \Lambda_{cR}$ or $\Lambda_R \subseteq \Lambda_{sR2} \subseteq \Lambda_{sR1} \subseteq \Lambda_{cR}$
- $\sigma^2(\Lambda_R) = P_R$
- the relay uses the codebook $\mathcal{C}_R = \{\Lambda_{cR} \cap \mathcal{V}_R\}$ consisting of codewords \mathbf{t}_R . This codebook is of rate $R_R = \frac{1}{n} \log \left(\frac{V_R}{V_{cR}} \right) = \frac{1}{n} \log \left(\frac{V_1}{V_{c1}} \right)$ if $\Lambda_{c2} \subseteq \Lambda_{c1}$ and of rate $R_R = \frac{1}{n} \log \left(\frac{V_R}{V_{cR}} \right) = \frac{1}{n} \log \left(\frac{V_1}{V_{c2}} \right)$ if $\Lambda_{c1} \subseteq \Lambda_{c2}$. This rate R_R in turn fixes the choice of γ in Theorem 2.

- Λ_{sR1} and Λ_{sR2} are used to decode lists at the two destinations, and their relative nesting depends on V_{sR1} and V_{sR2} (or equivalently P_{sR1} and P_{sR2} as both are Rogers good) subject to $V_R \geq V_{sR1} \geq V_{cR}$ and $V_{cR} \geq V_{sR2} \geq V_R$ which will be specified in the course of the proof.

Encoding: We use Block Markov encoding. Messages $w_{1b} \in \{1, 2, \dots, 2^{nR_1}\}$ and $w_{2b} \in \{1, 2, \dots, 2^{nR_2}\}$ are the messages the two terminals wish to send in block b . Nodes 1 and 2 send $\mathbf{X}_1(w_{1b})$ and $\mathbf{X}_2(w_{2b})$:

$$\mathbf{X}_1(w_{1b}) = (\mathbf{t}_1(w_{1b}) - \mathbf{U}_1(b)) \mod \Lambda_1$$

$$\mathbf{X}_2(w_{2b}) = (\mathbf{t}_2(w_{2b}) - \mathbf{U}_2(b)) \mod \Lambda_2,$$

for dithers $\mathbf{U}_1(b), \mathbf{U}_2(b)$ known to all nodes which are i.i.d. uniformly distributed over \mathcal{V}_1 and \mathcal{V}_2 and vary from block to block. At the relay, we assume that it has obtained

$$\mathbf{T}(b-1) = (\mathbf{t}_1(w_{1(b-1)}) + \mathbf{t}_2(w_{2(b-1)}) - Q_2(\mathbf{t}_2(w_{2(b-1)}) + \mathbf{U}_2(b-1))) \mod \Lambda_1 \quad (4.29)$$

in block $b-1$. Note that $\mathbf{T}(b-1)$ lies in $\{\Lambda_{c2} \cap \mathcal{V}_1\}$ if $\Lambda_{c1} \subseteq \Lambda_{c2}$ and in $\{\Lambda_{c1} \cap \mathcal{V}_1\}$ if $\Lambda_{c2} \subseteq \Lambda_{c1}$, and is furthermore uniformly distributed over this set consisting of 2^{nR_R} points. We may thus associate each $\mathbf{T}(b-1)$ with an index say $i(\mathbf{T}(b-1))$, which the relay then uses as index for the codeword $\mathbf{t}_R(i(\mathbf{T}(b-1)))$ in \mathcal{C}_R (also of rate R_R). To simplify notation and with some abuse of

notation we write $\mathbf{t}_R(\mathbf{T}(b-1))$ instead of the indexed version $\mathbf{t}_R(i(\mathbf{T}(b-1)))$. The relay then sends

$$\mathbf{X}_R(\mathbf{T}(b-1)) = (\mathbf{t}_R(\mathbf{T}(b-1)) + \mathbf{U}_R(b-1)) \mod \Lambda_R, \quad (4.30)$$

for $\mathbf{U}_R(b-1)$ a dither known to all nodes which is uniformly distributed over \mathcal{V}_R .

Decoding: During block b , the following messages / signals are known / decoded at each node:

- Node 1: knows $w_{11}, \dots, w_{1b}, w_{21}, w_{22}, \dots, w_{2(b-2)}$, decodes $w_{2(b-1)}$
- Node 2: knows $w_{21}, \dots, w_{2b}, w_{11}, w_{12}, \dots, w_{1(b-2)}$, decodes $w_{1(b-1)}$
- Node R : knows $\mathbf{T}(1), \mathbf{T}(2), \dots, \mathbf{T}(b-1)$, decodes $\mathbf{T}(b)$

Relay decoding: The relay terminal receives $\mathbf{Y}_R(b) = \mathbf{X}_1(w_{1b}) + \mathbf{X}_2(w_{2b}) + \mathbf{Z}_R(b)$, and, following the arguments of (1; 3; 2) can decode $\mathbf{T}(b) = (\mathbf{t}_1(w_{1b}) + \mathbf{t}_2(w_{2b}) - Q_2(\mathbf{t}_2(w_{2b}) + \mathbf{U}_2(b))) \mod \Lambda_1$ if

$$R_1 \leq \left[\frac{1}{2} \log \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N_R} \right) \right]^+, \quad R_2 \leq \left[\frac{1}{2} \log \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N_R} \right) \right]^+.$$

Terminal 2 decoding: Terminal 2 decodes $w_{1(b-1)}$ after block b from the received signals

$$\mathbf{Y}_2(b-1) = \mathbf{X}_R(\mathbf{T}(b-2)) + h_{12}\mathbf{X}_1(w_{1(b-1)}) + \mathbf{Z}_2(b-1)$$

$$\mathbf{Y}_2(b) = \mathbf{X}_R(\mathbf{T}(b-1)) + h_{12}\mathbf{X}_1(w_{1b}) + \mathbf{Z}_2(b).$$

This will generally follow the lattice version of regular encoding/sliding-window decoding scheme as described in Section 4.2. That is, after block $b-1$, terminal 2 first forms $\mathbf{Y}_2^*(b-1) = \mathbf{Y}_2(b-$

$1) - \mathbf{X}_R(\mathbf{T}(b-2))$ since it has decoded $w_{1(b-2)}$ and knows its own $w_{2(b-2)}$ and hence may form $\mathbf{X}_R(\mathbf{T}(b-2))$. Then it uses the list decoder of Theorem 3 to produce a list of messages $w_{1(b-1)}$, denoted by $L_{1-2}^{w_{1(b-1)}}(\mathbf{Y}_2^*(b-1))$, of size $2^{n(R_1 - C(h_{12}^2 P_1 / N_2))}$ using the lattice Λ_{s1} , whose fundamental Voronoi region volume is selected to asymptotically approach $V_{s1} = \left(\frac{N_2}{h_{12}^2 P_1 + N_2}\right)^{n/2} V_1$ (in the sense of (Equation 4.20)). For R approaching $\frac{1}{2} \log \left(1 + \frac{h_{12}^2 P_1 + P_R}{N_2}\right)$, where list decoding is relevant, $V_{c1} = \left(\frac{N_2}{h_{12}^2 P_1 + P_R + N_2}\right)^{n/2} V_1$ asymptotically, and thus $V_{c1} < V_{s1} < V_1$ as needed. To resolve which codeword was actually sent, it intersects this list with another list $L_{R-2}^{w_{1(b-1)}}(\mathbf{Y}_2(b))$ of $w_{1(b-1)}$ obtained in this block b . This list $L_{R-2}^{w_{1(b-1)}}(\mathbf{Y}_2(b))$ of messages $w_{1(b-1)}$ is obtained from $\mathbf{Y}_2(b)$ using lattice list decoding with the lattice Λ_{sR2} whose fundamental Voronoi region volume is taken to asymptotically approach $V_{sR2} = \left(\frac{h_{12}^2 P_1 + N_2}{P_R + h_{12}^2 P_1 + N_2}\right)^{n/2} V_R$. For R approaching $\frac{1}{2} \log \left(1 + \frac{h_{12}^2 P_1 + P_R}{N_2}\right)$, where list decoding is relevant, $V_{cR} = \left(\frac{N_2}{h_{12}^2 P_1 + P_R + N_2}\right)^{n/2} V_R$ asymptotically, and thus $V_{cR} < V_{sR2} < V_R$ as needed. One may verify that by construction of the nested lattice chains, all conditions of Theorem 3 are met. This list of messages $w_{1(b-1)}$ is actually obtained from decoding a list of $\mathbf{t}_R(\mathbf{T}(b-1))$, and using knowledge of its own $\mathbf{t}_2(w_{2(b-1)})$ to obtain a list of $\mathbf{t}_1(w_{1(b-1)})$ (and hence $w_{1(b-1)}$ by one-to-one mapping) of size approximately $2^{n(R_1 - C(\frac{P_R}{h_{12}^2 P_1 + N_2}))}$. To see this, notice that each \mathbf{t}_R is associated with a single $\mathbf{T} = (\mathbf{t}_1 + \mathbf{t}_2 - Q_2(\mathbf{t}_2 + \mathbf{U}_2)) \bmod \Lambda_1$. Then, given \mathbf{T} and \mathbf{t}_2 , one may obtain a single \mathbf{t}_1 as follows:

$$\begin{aligned}
& (\mathbf{T} - \mathbf{t}_2 + Q_2(\mathbf{t}_2 + \mathbf{U}_2)) \bmod \Lambda_1 \\
&= ((\mathbf{t}_1 + \mathbf{t}_2 - Q_2(\mathbf{t}_2 + \mathbf{U}_2)) - \mathbf{t}_2 + Q_2(\mathbf{t}_2 + \mathbf{U}_2)) \bmod \Lambda_1 \\
&= \mathbf{t}_1 \bmod \Lambda_1 = \mathbf{t}_1.
\end{aligned} \tag{4.31}$$

Similarly, given a \mathbf{T} and \mathbf{t}_1 one may obtain a single \mathbf{t}_2 as

$$\begin{aligned}
& (\mathbf{T} \bmod \Lambda_2 - \mathbf{t}_1) \bmod \Lambda_2 \\
&= ((\mathbf{t}_1 + \mathbf{t}_2 - Q_2(\mathbf{t}_2 + \mathbf{U}_2)) \bmod \Lambda_1 \bmod \Lambda_2 - \mathbf{t}_1) \bmod \Lambda_2 \\
&\stackrel{(a)}{=} ((\mathbf{t}_1 + \mathbf{t}_2 - Q_2(\mathbf{t}_2 + \mathbf{U}_2)) \bmod \Lambda_2 - \mathbf{t}_1) \bmod \Lambda_2 \\
&= \mathbf{t}_2 \bmod \Lambda_2 = \mathbf{t}_2,
\end{aligned} \tag{4.32}$$

where (a) follows from $\mathbf{X} \bmod \Lambda_1 \bmod \Lambda_2 = \mathbf{X} \bmod \Lambda_2$ when $\Lambda_1 \subseteq \Lambda_2$. Hence, the list of decoded codewords \mathbf{t}_R may be transformed into a list of \mathbf{t}_1 at Terminal node 2, which may in turn be associated with a list of $w_{1(b-1)}$. The two decoded lists of $w_{1(b-1)}$ are independent due to the independent mapping relationships between w_1 and \mathbf{t}_1 at Node 1 and between \mathbf{T} and

\mathbf{t}_R at the relay. List decoding ensures that at least the correct message lies in the intersection with high probability. To ensure no more than one in the intersection,

$$\begin{aligned} R_1 &< C(P_R/(h_{12}^2 P_1 + N_2)) + C(h_{12}^2 P_1/N_2) \\ &= C((h_{12}^2 P_1 + P_R)/N_2). \end{aligned}$$

Analogous steps apply to rate R_2 .

4.4.1 Comparison to existing rate regions

We briefly compare the new achievable rate region of Theorem 9 with three other existing Decode-and-Forward based rate regions for the two-way relay channel with direct links, and to the cut-set outer bound. In particular, in Figure 9, the region “Rankov-DF” (60, Proposition 2), the blue “Xie” (59, Theorem 3.1 under Gaussian inputs) and our orange “This work” (Theorem 9) are compared to the green cut-set outer bound under three different choices of noise and power constraints for $h_{12} = h_{21} = 1$. The “Rankov-DF” and “Xie” schemes use a multiple access channel model to decode the two messages at the relay, while we use lattice codes to decode their sum, which avoids the sum rate constraint. In the broadcast phase, the “Rankov-DF” scheme broadcasts the superposition of the two codewords, while the “Xie” and our scheme use a random binning technique to broadcast the bin index. The advantage of the “Rankov-DF” scheme is its ability of obtain a coherent gain at the receiver from the source and relay at the cost of a reduced power for each message (power split αP and $(1 - \alpha)P$). On the other hand, the “Xie” and Theorem 9 schemes both broadcast the bin index using all of the relay power,

but are unable to obtain coherent gains. We note that our current scheme does not allow for a coherent gain between the direct and relayed links as 1) we decode the sum of codewords and re-encode that, and 2) we use the full relay power to transmit this sum. Whether simultaneous coherent gains are possible to the two receivers while using a lattice-based scheme to decode the sum of codewords is an interesting open question which may possibly be addressed along the lines of (61).

At low SNR, the rate-gain seen by decoding the sum and eliminating the sum-rate constraint is outweighed by 1) the loss seen in the rates $\frac{1}{2} \log \left(\frac{P_i}{P_1+P_2} + SNR \right)$ compared to $\frac{1}{2} \log(1+SNR)$, or 2) the coherent gain present in the “Rankov-DF” scheme. At high SNR, our scheme performs well, and at least in some cases, is able to guarantee an improved finite-gap result to the outer bound, as further elaborated upon in (62). Further note that, compared with the two-way relay channel without direct links (2; 3), the direct links may provide additional information which translate to rate gains – direct comparison shows that the rate region in (3, Theorem 1) is always contained in that of Theorem 9.

4.5 The AWGN multiple-access relay channel

We now consider a second example of a relay network with two messages and cooperative relay links: the multiple-access relay channel (MARC). The MARC was proposed and studied in (10; 41; 42), and describes a multi-user communication scenario in which two users transmit different messages to the same destination with the help of a relay. As in the TWRC, the

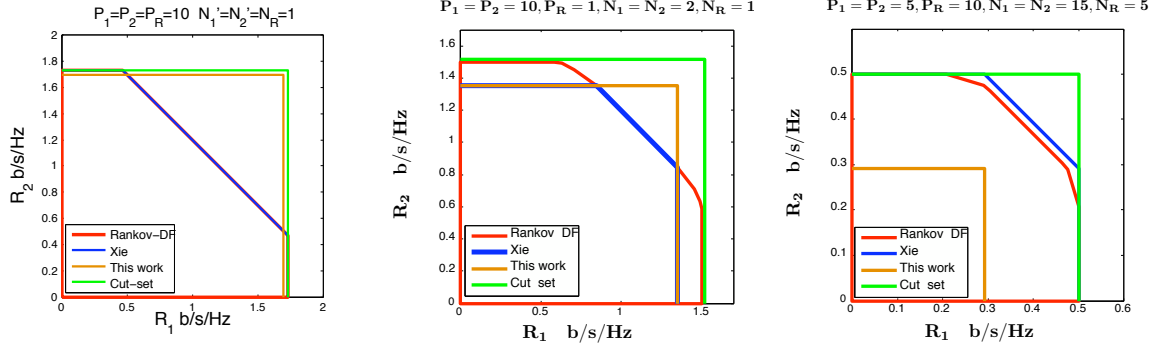


Figure 9. Comparison of decode-and-forward achievable rate regions of various two-way relay channel rate regions.

MARC can be seen as another example of an extension of the three-node relay channel. The channel model is described by

$$\mathbf{Y}_R = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}_R, \quad \mathbf{Z}_R \sim \mathcal{N}(\mathbf{0}, N_R \mathbf{I})$$

$$\mathbf{Y}_D = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_D + \mathbf{Z}_D, \quad \mathbf{Z}_D \sim \mathcal{N}(\mathbf{0}, N_D \mathbf{I}).$$

where \mathbf{X}_1 , \mathbf{X}_2 and \mathbf{X}_R have power constraints P_1 , P_2 and P_R .

An $(2^{nR_1}, 2^{nR_2}, n)$ code for the multiple access relay channel consists of the two sets of messages w_i , $i = 1, 2$ uniformly distributed over $\mathcal{M}_i := \{1, 2, \dots, 2^{nR_i}\}$, and two encoding functions $X_i^n : \mathcal{M}_i \rightarrow \mathbb{R}^n$ (shortened to \mathbf{X}_i) satisfying the power constraints P_i , a set of relay functions $\{f_j\}_{j=1}^n$ such that the relay channel input at time j is a function of the previously received relay channel outputs from channel uses 1 to $j-1$, $X_{R,j} = f_j(Y_{R,1}, \dots, Y_{R,j-1})$, and one decoding functions $g : \mathcal{Y}^n \rightarrow \mathcal{M}_1 \times \mathcal{M}_2$ which yields the message estimates $(\hat{w}_1, \hat{w}_2) := g(Y^n)$. We define the

average probability of error of the code to be $P_{n,e} := \frac{1}{2^{n(R_1+R_2)}} \sum_{w_1 \in \mathcal{M}_1, w_2 \in \mathcal{M}_2} \Pr\{(\hat{w}_1, \hat{w}_2) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\}$. The rate pair (R_1, R_2) is then said to be achievable by the multiple access relay channel if, for any $\epsilon > 0$ and for sufficiently large n , there exists an $(2^{nR_1}, 2^{nR_2}, n)$ code such that $P_{n,e} < \epsilon$. The capacity region C of the multiple access relay channel is the supremum of the set of achievable rate pairs.

We derive a new achievable rate region whose achievability scheme combines the previously derived lattice DF scheme, and the linearity of lattice codes using lattice list decoding. In particular, we demonstrate how we may decode the sum of two lattice codewords at the relay rather than decoding the individual messages, eliminating the sum-rate constraint seen in i.i.d. random coding schemes. The relay then forwards a re-encoded version of this which may be combined with lattice list decoding at the destination to obtain a new rate region.

Theorem 10 *Lattices in the AWGN multiple access relay channel. For any $\alpha \in [0, 1]$, the following rates are achievable for the AWGN multiple access relay channel:*

$$\begin{aligned}
R_1 &< \alpha \min \left(\left[\frac{1}{2} \log \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{P_1}{P_2 + P_R + N_D} \right) \right) \\
&\quad + (1 - \alpha) \min \left(\left[\frac{1}{2} \log \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{P_1 + P_R}{N_D} \right) \right), \\
R_2 &< (1 - \alpha) \min \left(\left[\frac{1}{2} \log \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{P_2}{P_1 + P_R + N_D} \right) \right) \\
&\quad + \alpha \min \left(\left[\frac{1}{2} \log \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N_R} \right) \right]^+, \frac{1}{2} \log \left(1 + \frac{P_2 + P_R}{N_D} \right) \right).
\end{aligned}$$

		Block 1	Block 2	Block 3	Block 4
Encoding:	①	$X_1(w_{11})$	$X_1(w_{12})$	$X_1(w_{13})$	$X_1(1)$
	②	$X_2(w_{21})$	$X_2(w_{22})$	$X_2(w_{23})$	$X_2(1)$
	①	$X_R(1)$	$X_R(T(1))$	$X_R(T(2))$	$X_R(T(3))$
Decoding:	①	$T(1)$	$T(2)$	$T(3)$	
	②	w_{11} $L_{2-D}^{w_{21}}$	w_{12} $L_{R-D}^{w_{21}} L_{2-D}^{w_{22}}$	w_{13} $L_{R-D}^{w_{22}} L_{2-D}^{w_{23}}$	$L_{R-D}^{w_{23}}$

Figure 10. Lattice Decode-and-Forward scheme for the AWGN multiple access relay channel.

Proof:

Codebook construction: We construct two nested lattice chains according to Theorem 2, $\Lambda_1, \Lambda_2, \Lambda_{s1}, \Lambda_{s2}, \Lambda_{c1}, \Lambda_{c2}$ and $\Lambda_R, \Lambda_{sR1}, \Lambda_{sR2}, \Lambda_{cR}$, nested in the exact same way as in the codebook construction of Theorem 9. **Encoding:** We again use block Markov encoding. At the b -th block, terminal 1 and 2 send $\mathbf{X}_1(w_{1b})$ and $\mathbf{X}_2(w_{2b})$, where

$$\mathbf{X}_1(w_{1b}) = (\mathbf{t}_1(w_{1b}) - \mathbf{U}_1(b)) \mod \Lambda_1$$

$$\mathbf{X}_2(w_{2b}) = (\mathbf{t}_2(w_{2b}) - \mathbf{U}_2(b)) \mod \Lambda_2.$$

At the relay, we assume that it has decoded

$$\mathbf{T}(b-1) = (\mathbf{t}_1(w_{1(b-1)}) + \mathbf{t}_2(w_{2(b-1)}) - Q_2(\mathbf{t}_2(w_{2(b-1)}) + \mathbf{U}_2(b-1)) \mod \Lambda_1$$

in block $b-1$. Following the exact same steps as in between (Equation 4.29) and (Equation 4.30), the relay sends

$$\mathbf{X}_R(\mathbf{T}(b-1)) = (\mathbf{t}_R(\mathbf{T}(b-1)) - \mathbf{U}_R(b-1)) \mod \Lambda_R.$$

The dithers $\mathbf{U}_1(b)$, $\mathbf{U}_2(b)$, and $\mathbf{U}_R(b)$ are known to all nodes and are i.i.d. and uniformly distributed over \mathcal{V}_1 , \mathcal{V}_2 , and \mathcal{V}_R and vary from block to block. In the first block 1, terminal 1 and terminal 2 send $\mathbf{X}_1(w_{11})$ and $\mathbf{X}_2(w_{21})$ respectively, while the relay sends a known $\mathbf{X}_R(1)$.

Decoding: At the end of each block b , the relay terminal receives $\mathbf{Y}_R(b) = \mathbf{X}_1(w_{1b}) + \mathbf{X}_2(w_{2b}) + \mathbf{Z}_R(b)$ and decodes $\mathbf{T}(b) = (\mathbf{t}_1(w_{1b}) + \mathbf{t}_2(w_{2b}) - Q_2(\mathbf{t}_2(w_{2b}) + \mathbf{U}_2(b)) \mod \Lambda_1$ as long as

$$R_1 \leq \left[\frac{1}{2} \log \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N_R} \right) \right]^+, \quad R_2 \leq \left[\frac{1}{2} \log \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N_R} \right) \right]^+$$

following arguments similar to those in (3).

The destination receives $\mathbf{Y}_D(b) = \mathbf{X}_1(w_{1b}) + \mathbf{X}_2(w_{2b}) + \mathbf{X}_R(\mathbf{T}(b-1)) + \mathbf{Z}_D(b)$ and either decodes the messages in the order w_{1b} and then $w_{2(b-1)}$ or the reverse w_{2b} and then $w_{1(b-1)}$. We describe the former; the latter follows analogously and we time-share between the two decoding

orders. The destination first decodes w_{1b} from $\mathbf{Y}_D(b)$, treating $\mathbf{X}_2(w_{2b}) + \mathbf{X}_R(\mathbf{T}(b-1)) + \mathbf{Z}_D(b)$ as noise. This equivalent noise is the sum of signals uniformly distributed over fundamental Voronoi regions of Rogers good lattices and Gaussian noise. Hence, according to Lemma 6, the probability of error in decoding the correct (unique) w_{1b} will decay exponentially as long as

$$R_1 < C \left(\frac{P_1}{P_2 + P_R + N_D} \right).$$

It then subtracts $\mathbf{X}_1(w_{1b})$ from the signal $\mathbf{Y}_D(b)$ to obtain $\mathbf{Y}_D^*(b) = \mathbf{X}_2(w_{2b}) + \mathbf{X}_R(\mathbf{T}(b-1)) + \mathbf{Z}_D(b)$ and decodes a list of $w_{2(b-1)}$ denoted by $L_{R-D}^{w_{2(b-1)}}(\mathbf{Y}_D^*(b))$ of size $2^{n(R_2 - C(\frac{P_R}{P_2 + N_D}))}$ assuming side information $w_{1(b-1)}$, and treating $\mathbf{X}_2(w_{2b}) + \mathbf{Z}_D(b)$ as noise. This list of $w_{2(b-1)}$ is obtained from a lattice list decoder based on $\mathbf{t}_R(\mathbf{T}(b-1))$ and noting the one-to-one correspondence between $\mathbf{t}_R(\mathbf{T}(b-1))$ and $\mathbf{t}_2(w_{2(b-1)})$ and hence $w_{2(b-1)}$ given $\mathbf{t}_1(w_{1(b-1)})$, using the arguments of (Equation 4.31) and (Equation 4.33).

The destination then intersects the list $L_{R-D}^{w_{2(b-1)}}(\mathbf{Y}_D^*(b))$ with another list $L_{2-D}^{w_{2(b-1)}}(\mathbf{Y}_D^*(b-1))$ of size $2^{n(R_2 - C(\frac{P_2}{N_D}))}$ obtained in the block $b-1$ (described next for block b) to determine the unique $w_{2(b-1)}$. Once the destination has decoded w_{1b} , $w_{2(b-1)}$ and $w_{1(b-1)}$, it is also able to reconstruct $\mathbf{X}_R(\mathbf{T}(b-1))$.

At last, the destination decodes a list $L_{2-D}^{w_{2b}}(\mathbf{Y}_D^*(b))$ of possible w_{2b} of size $2^{n(R_2 - C(\frac{P_2}{N_D}))}$ from the signal $\mathbf{Y}_D^*(b) = \mathbf{Y}_D(b) - \mathbf{X}_1(w_{1b}) - \mathbf{X}_R(\mathbf{T}(b-1)) = \mathbf{X}_2(w_{2b}) + \mathbf{Z}_D(b)$ which is used

to determine w_{2b} in the next block $b + 1$. To ensure that there is a unique codeword $w_{2(b-1)}$ in the intersection of the two lists $L_{R-D}^{w_{2(b-1)}}(\mathbf{Y}_D^*(b))$ and $L_{2-D}^{w_{2(b-1)}}(\mathbf{Y}_D^*(b-1))$, we need

$$R_2 < C\left(\frac{P_R}{P_2 + N_D}\right) + C\left(\frac{P_2}{N_D}\right) = \frac{1}{2} \log\left(1 + \frac{P_2 + P_R}{N_D}\right).$$

We presented the decoding order $w_{1b}, w_{2(b-1)}$. Alternatively, one may decode in the order w_{2b} and $w_{1(b-1)}$ at the analogous rates.

Time sharing with parameter $0 \leq \alpha \leq 1$ between the orders yields the theorem.

Remark 4 *Note that the above region is derived using time-sharing between two decoding orders at the destination. This results as we employ successive decoding at the destination in order to allow for the use of lower complexity Euclidean lattice decoding, rather than a more complex form of “joint” decoding for lattices proposed for example in (5; 63). Further note that this region does not always outperform or even attain the same rates as random coding based schemes – in fact, as in the two-way relay channel, there is a trade off between rate gains from decoding the sum at the relay node, and coherent gains and joint decoding at the destination.*

4.6 Lattice Dirty-Paper Coding in Simple Relay Channel

This section considers a toy example where a lattice Dirty-Paper Coding technique can be used in a simple relaying scenario. A two-hop S-R-D Gaussian network is considered with a source (S), a relay (R) and a destination (D) where there is no direct link between S and D. The destination node experiences additive interference which is known to the source node. This noise renders the channel state-dependent. In this case, one would hope to exploit this

knowledge of the channel state at the source node to obtain a “clean” or interference-free channel, just as Costa’s dirty-paper coding does for one-hop channels with state non-causally known to the transmitter. We demonstrate a scheme which achieves to within $\frac{1}{2}$ bit of a “clean” channel. This novel scheme is based on a nested-lattice code and a Decode-and-Forward (DF) relay. Intuitively, this strategy uses the structure provided by nested lattice codes to cancel the “integer” (or lattice quantized) part of the interference and treats the “residual” (or quantization noise) as noise. This result can be seen as a straight-forward extension of lattice Dirty-Paper Coding in (18) where the source pre-codes the known interference so that the interference may be cancelled at the destination.

4.6.1 Channel Model

We consider an AWGN two-hop channel model with interference, as shown on the right hand side of Figure 14. In particular, the model consists of three nodes, the “source” or Tx, node 1; the “relay” node 2, and the “destination” or Rx, node 3. The channel inputs of nodes 1 and 2 are denoted by X_1 and X_2 , taking on values $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$ subject to average power constraints $E[|X_1|^2] \leq P_1$ and $E[|X_2|^2] \leq P_2$. The received signals at node 2 and 3 respectively are Y_2 and Y_3 , taking on values $y_2 \in \mathcal{Y}_2$ and $y_3 \in \mathcal{Y}_3$. We will communicate over n channel uses and we let $X_1^n := (X_1(1), X_1(2), \dots, X_1(n))$ where $X_1(k)$ denotes the input at channel use k (and

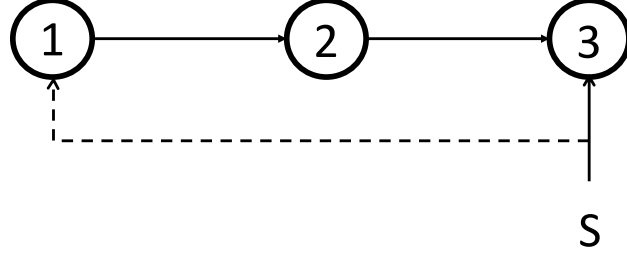


Figure 11. Interference S is experienced at the destination but only known at the source.

similarly for X_2^n, Y_2^n, Y_3^n . We consider two-hop AWGN networks with arbitrary interference S^n , where, at channel use k , the inputs and outputs of the channels are related as

$$Y_2(k) = X_1(k) + Z_2(k), \text{ Tx 1 knows } S(k)$$

$$Y_3(k) = X_2(k) + S(k) + Z_3(k),$$

where for notational convenience, it is assumed that power constraints of the source and relay are 1, i.e. $P_1 = P_2 = 1$, and the noise is AWGN with $Z_2(k) \sim \mathcal{N}(0, \frac{1}{S_1})$ and $Z_3(k) \sim \mathcal{N}(0, \frac{1}{S_2})$ respectively. This ensures that, in the absence of interference S , the link $1 \rightarrow 2$ has capacity

$\frac{1}{2} \log(1+S_1)$ and the link $2 \rightarrow 3$ has capacity $\frac{1}{2} \log(1+S_2)$. In this channel, we wish to transmit a message $w \in \{1, 2, \dots, 2^{nR}\}$ at rate $R > 0$ from node 1 to node 3 (which forms an estimate \hat{w} of w from its received signal Y_3^n) such that $\Pr\{\hat{w} \neq w\} \rightarrow 0$ as the number of channel uses, $n \rightarrow \infty$. From now on, to simplify notation, we will abuse notation slightly and drop the superscript n , using X_1 to denote X_1^n for the remainder, as we will always be dealing with n channel uses.

4.6.2 Lattice Achievability

Theorem 11 *The following rate may be achieved using a structured nested-lattice coding based DF scheme*

$$R < \left[\frac{1}{2} \log \left(\frac{1}{\frac{1}{1+S_1} + \frac{1}{1+S_2}} \right) \right]^+ \quad (4.34)$$

$$= \left[\frac{1}{2} \log \left(\frac{S_1 S_2 + S_1 + S_2 + 1}{S_1 + S_2 + 2} \right) \right]^+, \quad (4.35)$$

where S_1 and S_2 are the signal-to-noise ratio for the two links: $1 \rightarrow 2$ and $2 \rightarrow 3$ respectively.

For the special case $S_1 = S_2 = S$, this reduces to $R < \frac{1}{2} \log \left(\frac{1}{2} + \frac{S}{2} \right)$.

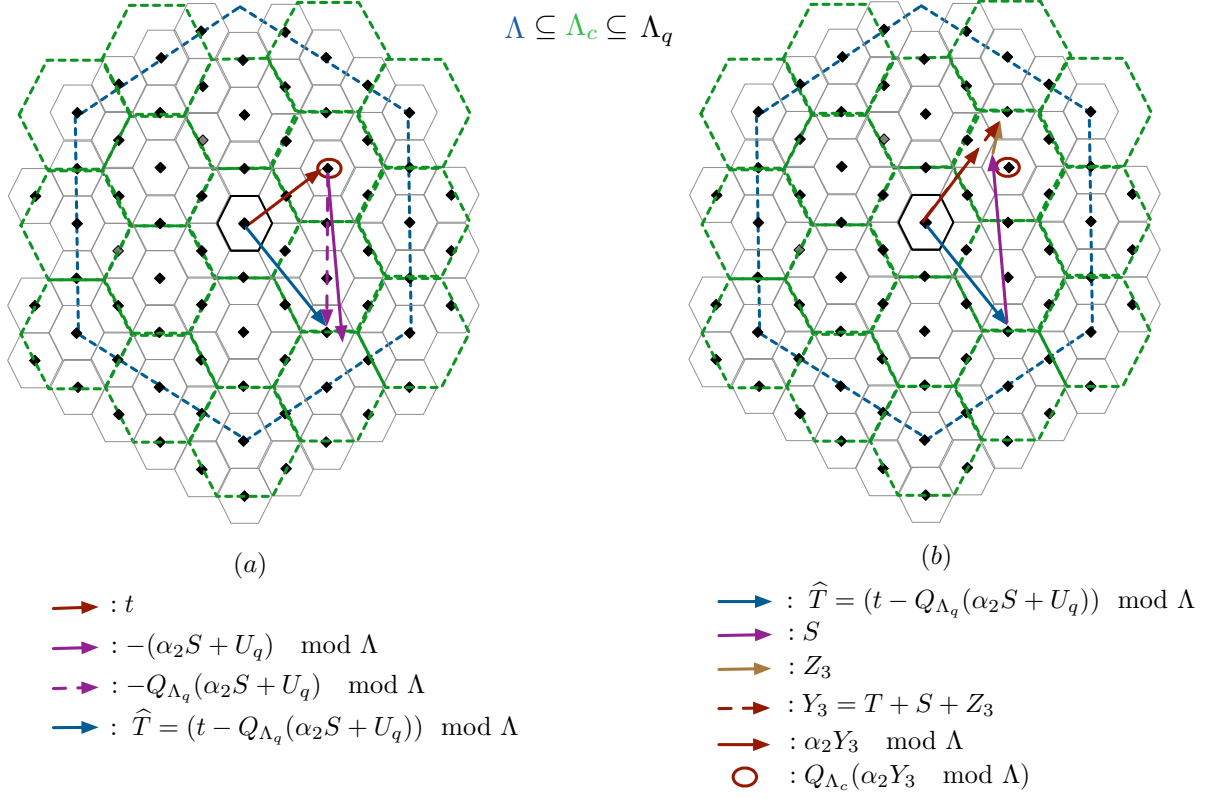


Figure 12. Illustration of key achievability steps: (a) interference “pre-cancellation” is performed at the transmitter Node 1 who knows the interference S , (b) the receiver Node 3 experiences interference S , and suffers from a quantization noise “residual”.

Remark: We note that the rate achieved in Theorem 11 achieves to within at most $\frac{1}{2}$ bit of the clean channel capacity which forms an outer bound for our channel model, as

$$\begin{aligned}
 \frac{1}{2} \log \left(\frac{1}{\frac{1}{1+S_1} + \frac{1}{1+S_2}} \right) + \frac{1}{2} &= \frac{1}{2} \log \left(\frac{1}{\frac{1}{2(1+S_1)} + \frac{1}{2(1+S_2)}} \right) \\
 &\geq \frac{1}{2} \log \left(\frac{1}{2 * \frac{1}{2(1+\min(S_1, S_2))}} \right) \\
 &= \frac{1}{2} \log (1 + \min(S_1, S_2)).
 \end{aligned}$$

Proof: We now prove Theorem 11. We consider a good nested lattice chain $\Lambda \subseteq \Lambda_c \subseteq \Lambda_q$, where we will specify the second moment / power constraints in the following. We need Λ and Λ_q to be both *Rogers good* and *Poltyrev good*, and Λ_c to be *Poltyrev good*. The existence of such a good lattice chain is provided in Section 3.3. The message coding rate is

$$R = \frac{1}{n} \log \left(\frac{V(\Lambda)}{V(\Lambda_c)} \right) = \frac{1}{2} \log \left(\frac{1}{\sigma^2(\Lambda_c)} \right).$$

The coding rate of $Q_{\Lambda_q}(\cdot) \bmod \Lambda$ is

$$R_q = \frac{1}{n} \log \left(\frac{V(\Lambda)}{V(\Lambda_q)} \right) = \frac{1}{2} \log \left(\frac{1}{\sigma^2(\Lambda_q)} \right).$$

Encoding at the source (Node 1): message $w \in \mathcal{W} = \{1, 2, \dots, 2^{nR}\}$ is one-to-one mapped to the lattice codeword $t \in \{\Lambda_c \cap \mathcal{V}(\Lambda)\}$ ($w \leftrightarrow t$). The transmitter chooses the t associated with transmitted message and sends

$$X_1 = (T + U_1) \bmod \Lambda$$

where $T = (t - Q_{\Lambda_q}(\alpha_2 S + U_q)) \bmod \Lambda$. U_q is the quantization dither which is uniformly distributed over $\mathcal{V}(\Lambda_q)$ and also known by the destination. Here U_1 is the channel coding dither which is uniformly distributed over $\mathcal{V}(\Lambda)$ and is known at the relay. The second moment of Λ is limited by the transmit power, which is assumed to be 1 in this case. This encoding

step is illustrated in Fig 4.6.2(a), where we see the pre-subtraction of the scaled and quantized interference S , all $\bmod \Lambda$.

Decoding at the relay (Node 2): the relay receives

$$Y_2 = X_1 + Z_2$$

and forms the following signal

$$\begin{aligned} Y'_2 &= (\alpha_1 X_1 + \alpha_1 Z_2 - U_1) \bmod \Lambda \\ &= (t - Q_{\Lambda_q}(\alpha_2 S + U_q) - (1 - \alpha_1)X_1 + \alpha_1 Z_2) \bmod \Lambda. \end{aligned}$$

Choosing $\alpha_1 = \alpha_{1opt} = \frac{S_1}{S_1+1}$, the relay can decode $\hat{T} = (t - Q_{\Lambda_q}(\alpha_2 S + U_q)) \bmod \Lambda$ with constraints:

$$R < \frac{1}{2} \log(1 + S_1), \tag{4.36}$$

$$R_q < \frac{1}{2} \log(1 + S_1). \tag{4.37}$$

according to Lemma 6. This implies that

$$R_q = \frac{1}{2} \log \left(\frac{1}{\sigma^2(\Lambda_q)} \right) < \frac{1}{2} \log(1 + S_1)$$

which results again in a lower bound on the quantization lattice's second moment

$$\sigma^2(\Lambda_q) > \frac{1}{1 + S_1}.$$

Encoding at the relay and decoding at the destination: the relay sends $X_2 = (T + U_2) \bmod \Lambda$ and the destination receives

$$Y_3 = X_2 + S + Z_3,$$

and uses an MMSE estimator to decode t by computing

$$\begin{aligned} Y'_3 &= (\alpha_2 Y_3 + U_q - U_2) \bmod \Lambda \\ &= (t - Q_{\Lambda_q}(\alpha_2 S + U_q) + U_2 - (1 - \alpha_2)X_2 \\ &\quad + \alpha_2 S + \alpha_2 Z_3 + U_q - U_2) \bmod \Lambda \\ &= (t - (\alpha_2 S - U_q) \bmod \Lambda_q - (1 - \alpha_2)X_2 + \alpha_2 Z_3) \bmod \Lambda \end{aligned}$$

where $(\alpha_2 S - U_q) \bmod \Lambda_q$ is a random variable independent of all others which is uniformly distributed over $\mathcal{V}(\Lambda_q)$. Thus, $-(\alpha_2 S - U_q) \bmod \Lambda_q$, $-(1 - \alpha_2)X_2$, and $\alpha_2 Z_3$ may be regarded as three independent noise terms with variances $\sigma^2(\Lambda_q)$, $(1 - \alpha_2)^2$ and $\alpha_2^2 \frac{1}{S_2}$, and approximated as Gaussian noise as in (25) when $n \rightarrow \infty$. In this last decoding step we see the effect of the interference “pre-cancellation” at Node 1, as illustrated in Figure 4.6.2(b). In the Figure, the

effect of the dithers is dropped for clarity and illustration purposes only, and is technically still required. Choosing $\alpha_2 = \alpha_{2opt} = \frac{S_2}{S_2+1}$, the destination can decode t when

$$R < \frac{1}{2} \log \left(\frac{1}{\frac{1}{1+S_2} + \sigma^2(\Lambda_q)} \right) \quad (4.38)$$

$$< \frac{1}{2} \log \left(\frac{1}{\frac{1}{1+S_2} + \frac{1}{1+S_1}} \right) \quad (4.39)$$

$$= \frac{1}{2} \log \left(\frac{S_1 S_2 + S_1 + S_2 + 1}{S_1 + S_2 + 2} \right). \quad (4.40)$$

Observe that the constraint (Equation 4.36) is always looser than the constraint (Equation 4.38).

CHAPTER 5

LATTICE CODING FOR COMPRESS-AND-FORWARD IN SINGLE RELAY CHANNEL

We have shown several lattice based Decode-and-Forward schemes for relay networks. Forcing the relay(s) to decode the message(s) they do not need imposes a rate constraint; Compress-and-Forward (CF) is an alternative type of forwarding which alleviates this constraint. Cover and El Gamal first proposed a CF scheme for the relay channel in (8) in which the relay does not decode the message but instead compresses its received signal and forwards the compression index. The destination first recovers the compressed signal, using its direct-link side-information (the Wyner-Ziv problem of lossy source coding with correlated side-information at the receiver), and then proceeds to decode the message from the recovered compressed signal and the received signal.

It is natural to wonder whether lattice codes may be used in the original Cover and El Gamal CF scheme for the relay channel. We answer this in the positive. We note that lattices have recently been shown to achieve the Quantize-Map-and-Forward rates for general relay channels using Quantize-and-Map scheme (similar to the CF scheme) which quantizes the received signal at the relay and re-encodes it without any form of binning / hashing in (5). The contribution in this section is to show an alternative achievability scheme which achieves the same rate in the three node relay channel, demonstrating that lattices may be used to achieve CF-based rates

in a number of fashions. We note that our decoder employs a lattice decoder rather than the more complex joint typicality, or “consistency check” decoding of (5).

In the CF scheme of (8), Wyner-Ziv coding – which exploits binning – is used at the relay to exploit receiver side-information obtained from the direct link between the source and destination. The usage of lattices and structured codes for binning (as opposed to their random binning counterparts) was considered in a comprehensive fashion in (18). Of particular interest to the problem considered here is the nested lattice-coding approach of (18) to the Gaussian Wyner-Ziv coding problem.

5.1 Lattice codes for the Wyner-Ziv model in Compress-and-Forward

We consider the lossy compression of the Gaussian source $\mathbf{Y} = \mathbf{X} + \mathbf{Z}_1$, with Gaussian side-information $\mathbf{X} + \mathbf{Z}_2$ available at the reconstruction node, where \mathbf{X}, \mathbf{Z}_1 and \mathbf{Z}_2 are independent vectors of length n which are independent and each generated in an i.i.d. fashion according to a Gaussian of zero mean and variance P, N_1 , and N_2 , respectively. We use the same definitions for the channel model and for achievability as in Section 4.2. The rate-distortion function for the source $\mathbf{X} + \mathbf{Z}_1$ taking on values in $\mathcal{X}_1^n = \mathbb{R}^n$ with side-information $\mathbf{X} + \mathbf{Z}_2$ taking on values in $\mathcal{X}_2^n = \mathbb{R}^n$ is the infimum of rates R such that there exist maps $i_n : \mathcal{X}_1^n \rightarrow \{1, 2, \dots, 2^{nR}\}$ and $g_n : \mathcal{X}_2^n \times \{1, 2, \dots, 2^{nR}\} \rightarrow \mathcal{X}_1^n$ such that $\limsup_{n \rightarrow \infty} E[d(\mathbf{X} + \mathbf{Z}_1, g_n(\mathbf{X} + \mathbf{Z}_2, i_n(\mathbf{X} + \mathbf{Z}_1)))] \leq D$ for some distortion measure $d(\cdot, \cdot)$. If the distortion measure $d(\cdot, \cdot)$ is the squared error distortion,

$d(\mathbf{X}, \hat{\mathbf{X}}) = \frac{1}{n} E[\|\mathbf{X} - \hat{\mathbf{X}}\|^2]$, then, by (64), the rate distortion function $R(D)$ for the source $X + Z_1$ given the side-information $X + Z_2$ is given by

$$\begin{aligned} R(D) &= \frac{1}{2} \log \left(\frac{\sigma_{X+Z_1|X+Z_2}^2}{D} \right), & 0 \leq D \leq \sigma_{X+Z_1|X+Z_2}^2 \\ &= \frac{1}{2} \log \left(\frac{N_1 + \frac{PN_2}{P+N_2}}{D} \right), & 0 \leq D \leq N_1 + \frac{PN_2}{P+N_2}, \end{aligned}$$

and 0 otherwise, where $\sigma_{X+Z_1|X+Z_2}^2$ is the conditional variance of $X + Z_1$ given $X + Z_2$.

A general lattice code implementation of the Wyner-Ziv scheme is considered in (18). In order to mimic the CF scheme achieved by Gaussian random codes of (8), we need a slightly sub-optimal version of the optimal scheme described in (18). That is, in the context of CF, and to mimic the rate achieved by independent Gaussian random codes used for compression in the CF rate of (8), the quantization noise after compression should be independent of the signal to be compressed to allow for two independent views of the source, i.e. to express the compressed signal as $\hat{\mathbf{Y}} = \mathbf{Y} - \mathbf{E}_q = \mathbf{X} + \mathbf{Z}_1 - \mathbf{E}_q$ where \mathbf{E}_q is independent of $\mathbf{X} + \mathbf{Z}_1$. This may be achieved by selecting $\alpha_1 = 1$ in a modified version of the lattice-coding Wyner-Ziv scheme of (18) rather than the optimal MMSE scaling coefficient $\alpha_1 = \sqrt{1 - \frac{D}{N_1 + \frac{PN_2}{P+N_2}}}$. This roughly allows one to view $\hat{\mathbf{Y}} = \mathbf{X} + \mathbf{N}_1 - \mathbf{E}_q$ as an equivalent AWGN channel, and is the form generally used in Gaussian CF as in (11). Whether this is optimal is unknown. The second difference from direct application of (18) is that, in our lattice CF scheme, the signal \mathbf{X} is no longer Gaussian but uniformly distributed over the fundamental Voronoi region of a Rogers good lattice. We modify the scheme of (18) to incorporate these two changes next.

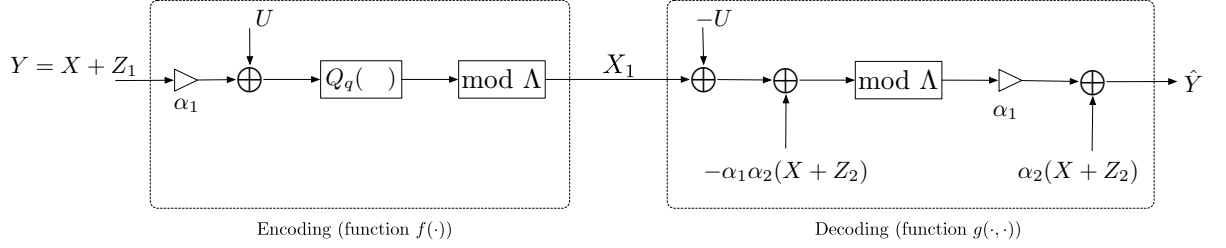


Figure 13. Lattice coding for the $(\mathbf{X} + \mathbf{Z}_1, \mathbf{X} + \mathbf{Z}_2)$ Wyner-Ziv problem.

Corollary 12 *Lattices for the $(\mathbf{X} + \mathbf{Z}_1, \mathbf{X} + \mathbf{Z}_2)$ Wyner-Ziv problem used in the lattice CF scheme based on (18). Let \mathbf{X} be uniformly distributed over the fundamental Voronoi region of a Rogers good lattice with second moment P , while $\mathbf{Z}_1 \sim \mathcal{N}(\mathbf{0}, N_1 \mathbf{I})$ and $\mathbf{Z}_2 \sim \mathcal{N}(\mathbf{0}, N_2 \mathbf{I})$. The following rate-distortion function for the lossy compression of the source $\mathbf{X} + \mathbf{Z}_1$ to be reconstructed as $\mathbf{X} + \mathbf{Z}_1 - \mathbf{E}_q$ (where \mathbf{E}_q is independent of $\mathbf{X} + \mathbf{Z}_1$ and has variance D) may be achieved using lattice codes:*

$$R(D) = \frac{1}{2} \log \left(1 + \frac{N_1 + \frac{PN_2}{P+N_2}}{D} \right), \quad 0 \leq D \leq \infty.$$

Proof: Consider a pair of nested lattice codes $\Lambda \subseteq \Lambda_q$, where Λ_q is Rogers-good with second moment D , and Λ is Poltyrev-good with second moment $N_1 + \frac{PN_2}{P+N_2} + D$. The existence of such a nested lattice pair good for quantization is guaranteed as in (18). We consider the encoding and decoding schemes of Figure Figure 13, similar to that of (18). We let \mathbf{U} be a quantization

dither signal which is uniformly distributed over \mathcal{V}_q and introduce the following coefficients (choices justified later):

$$\alpha_1 = 1, \quad \alpha_2 = \frac{P}{P + N_2}. \quad (5.1)$$

Encoding: The encoder quantizes the scaled and dithered signal $\alpha_1(\mathbf{X} + \mathbf{Z}_1) + \mathbf{U}$ to the nearest fine lattice point, which is then modulo-ed back to the coarse lattice fundamental Voronoi region as

$$\begin{aligned} \mathbf{I} &:= Q_q(\alpha_1(\mathbf{X} + \mathbf{Z}_1) + \mathbf{U}) \mod \Lambda \\ &= (\mathbf{X} + \mathbf{Z}_1 + \mathbf{U} - \mathbf{E}_q) \mod \Lambda. \end{aligned}$$

where $\mathbf{E}_q := (\mathbf{X} + \mathbf{Z}_1 + \mathbf{U}) \mod \Lambda_q$ is independent of $\mathbf{X} + \mathbf{Z}_1$ and uniformly distributed over \mathcal{V}_q according to the Crypto lemma (50). The encoder sends index i of \mathbf{I} at the source coding rate

$$R = \frac{1}{n} \log \left(\frac{V(\Lambda)}{V(\Lambda_q)} \right) = \frac{1}{2} \log \left(1 + \frac{N_1 + \frac{PN_2}{P+N_2}}{D} \right).$$

Decoding: The decoder receives the index i of \mathbf{I} and reconstructs $\hat{\mathbf{Y}}$ as

$$\begin{aligned}
\hat{\mathbf{Y}} &= \alpha_1((\mathbf{I} - \mathbf{U} - \alpha_1\alpha_2(\mathbf{X} + \mathbf{Z}_2)) \bmod \Lambda) + \alpha_2(\mathbf{X} + \mathbf{Z}_2) \\
&= \alpha_1((\alpha_1((1 - \alpha_2)\mathbf{X} - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q) \bmod \Lambda) + \alpha_2(\mathbf{X} + \mathbf{Z}_2) \\
&\stackrel{(a)}{=} \alpha_1(\alpha_1((1 - \alpha_2)\mathbf{X} - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q) + \alpha_2(\mathbf{X} + \mathbf{Z}_2) \\
&= \mathbf{X} + \mathbf{Z}_1 - \mathbf{E}_q
\end{aligned}$$

where equivalence (a) denotes asymptotic equivalence (as $n \rightarrow \infty$), since, as in (18, Proof of (4.19))

$$\Pr\{(\alpha_1((1 - \alpha_2)\mathbf{X} - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q) \bmod \Lambda \neq \alpha_1((1 - \alpha_2)\mathbf{X} - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q\} \rightarrow 0 \quad (5.2)$$

for a sequence of a good nested lattice codes since

$$\frac{1}{n}E\|\alpha_1((1 - \alpha_2)\mathbf{X} - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q\|^2 = \frac{PN_2}{P + N_2} + N_1 + D = \sigma^2(\Lambda). \quad (5.3)$$

Note that there is a slight difference from (18, Proof of (4.19)) since \mathbf{X} is uniformly distributed over the fundamental Voronoi region of a Rogers good lattice rather than Gaussian distributed. However, according to Lemma 5, $\alpha_1((1 - \alpha_2)\mathbf{X}_1 - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1) - \mathbf{E}_q = (1 - \alpha_2)\mathbf{X}_1 - \alpha_2\mathbf{Z}_2 + \mathbf{Z}_1 - \mathbf{E}_q$ may be upper bounded by the pdf of an i.i.d. Gaussian random vector (times a constant) with variance approaching (Equation 5.3) since \mathbf{X}_1 is uniformly distributed over the Rogers good

$\mathcal{V}_1, \mathbf{E}_q$ is uniformly distributed over the Rogers good \mathcal{V}_q of second moment D , and $-\alpha_2 \mathbf{Z}_2 + \mathbf{Z}_1$ is Gaussian. Then because Λ is Poltyrev good, (Equation 5.2) can be made arbitrary small as $n \rightarrow \infty$. This guarantees a distortion of D as \mathcal{V}_q is of second moment D .

5.2 Lattice coding for Compress-and-Forward

Armed with a lattice Wyner-Ziv scheme, we mimic every step of the CF scheme for the AWGN relay channel of Figure 5 and CF scheme described in (8) using lattice codes and will show that the same rate as that achieved using random Gaussian codebooks may be achieved in a structured manner.

Theorem 13 *Lattices achieve the CF rate for the relay channel. The following rate may be achieved for the AWGN relay channel using lattice codes in a lattice Compress-and-Forward fashion:*

$$R < \frac{1}{2} \log \left(1 + \frac{P}{N_D} + \frac{PP_R}{PN_R + PN_D + P_R N_R + N_R N_D} \right).$$

Proof:

Lattice codebook construction: We employ three nested lattice pairs of dimension n satisfying:

- Channel codebook for Node S : codewords $\mathbf{t}_1 \in \mathcal{C}_1 = \{\Lambda_{c1} \cap \mathcal{V}_1\}$ where $\Lambda_1 \subseteq \Lambda_{c1}$, and Λ_1 is both Rogers-good and Poltyrev-good and Λ_{c1} is Poltyrev-good. We set $\sigma^2(\Lambda_1) = P$ to satisfy the transmitter power constraint. We associate each message $w \in \{1, 2, \dots, 2^{nR}\}$ with a code-

word $\mathbf{t}_1(w)$ in one-to-one fashion and send a dithered version of $\mathbf{t}_1(w)$. Note that Λ_{c1} is chosen such that $|\mathcal{C}_1| = 2^{nR}$.

- Channel codebook for the relay: codewords $\mathbf{t}_R \in \mathcal{C}_R = \{\Lambda_{cR} \cap \mathcal{V}_R\}$ where $\Lambda_R \subseteq \Lambda_{cR}$, and Λ_R is both Rogers-good and Poltyrev-good and Λ_{cR} is Poltyrev-good. We set $\sigma^2(\Lambda_R) = P_R$ to satisfy the relay power constraint. We associate each compression index $i \in \{1, 2, \dots, 2^{nR'}\}$ with the codeword $\mathbf{t}_R(i)$ in a one-to-one fashion and send a dithered version of $\mathbf{t}_R(i)$. Note that Λ_{cR} is chosen such that $|\mathcal{C}_R| = 2^{nR'}$.

- Quantization/Compression codebook: $\mathbf{t}_q \in \mathcal{C}_q = \{\Lambda_q \cap \mathcal{V}\}$ and $\Lambda \subseteq \Lambda_q$, where Λ is Poltyrev-good and Λ_q is Rogers-good. We set $\sigma^2(\Lambda_q) = D$, $\sigma^2(\Lambda) = N_R + \frac{P_1 N_2}{P_1 + N_2} + D$, such that the source coding rate is $\hat{R} = \frac{1}{n} \log \left(\frac{V(\Lambda)}{V(\Lambda_q)} \right) = \frac{1}{2} \log \left(1 + \frac{N_R + \frac{P_1 N_2}{P_1 + N_2}}{D} \right)$.

Encoding: We use block Markov encoding as (8). In block b , Node 1 transmits

$$\mathbf{X}_S(w_b) = (\mathbf{t}_1(w_b) + \mathbf{U}_1(b)) \mod \Lambda_1,$$

where $\mathbf{U}_1(b)$ is the dither uniformly distributed over \mathcal{V}_1 . The relay quantizes the received signal in the previous block $b - 1$,

$$\mathbf{Y}_R(b - 1) = \mathbf{X}_S(w_{b-1}) + \mathbf{Z}_R(b - 1)$$

to $\mathbf{I}(w_{b-1}) = Q_q(\mathbf{X}_S(w_{b-1}) + \mathbf{Z}_R(b - 1) + \mathbf{U}_q - \mathbf{E}_q) \mod \Lambda$ (with index $i(w_{b-1})$) by using the quantization lattice code pair (Λ_q, Λ) as described in the encoding part of Theorem 12, for \mathbf{U}_q a quantization dither uniformly distributed over \mathcal{V}_q and $\mathbf{E}_q := (\mathbf{X}_S(w_{b-1}) + \mathbf{Z}_R(b - 1) + \mathbf{U}_q)$

mod Λ_q . Node 2 chooses the codeword $\mathbf{t}_R(i(w_{b-1}))$ associated with the index $i(w_{b-1})$ of $\mathbf{I}(w_{b-1})$ and sends

$$\mathbf{X}_R(w_{b-1}) = (\mathbf{t}_R(i(w_{b-1})) + \mathbf{U}_R(b-1)) \mod \Lambda$$

with $\mathbf{U}_R(b-1)$ the dither signal uniformly distributed over \mathcal{V}_R and independent across blocks.

Decoding: In block b , Node D receives

$$\mathbf{Y}_D(b) = \mathbf{X}_S(w_b) + \mathbf{X}_R(w_{b-1}) + \mathbf{Z}_D(b).$$

It first decodes w_{b-1} using lattice decoding as in (25) or Lemma 6 as long as

$$R' < \frac{1}{2} \log \left(1 + \frac{P_R}{P + N_D} \right).$$

We note that the source coding rate of \mathbf{I} , \hat{R} must be less than the channel coding rate R' , i.e.

$$\frac{1}{2} \log \left(1 + \frac{N_R + \frac{PN_D}{P+N_D}}{D} \right) < \frac{1}{2} \log \left(1 + \frac{P_R}{P + N_D} \right), \quad (5.4)$$

which sets a lower bound on the achievable distortion D . Node D then may obtain

$$\mathbf{Y}'_D(b) = \mathbf{Y}_D(b) - \mathbf{X}_R(w_{b-1}) = \mathbf{X}_S(w_b) + \mathbf{Z}_D(b)$$

which is used as direct-link side-information in the next block $b+1$. In the previous block, Node D had also obtained $\mathbf{Y}'_D(b-1) = \mathbf{X}_S(w_{b-1}) + \mathbf{Z}_D(b-1)$. Combining this with $\mathbf{I}(w_{b-1})$, Node

D uses $\mathbf{Y}'_D(b-1)$ as side-information to reconstruct $\widehat{\mathbf{Y}}_D(b-1)$ as in the decoder of Theorem 12.

Thus, we see that the CF scheme employs the $(\mathbf{X} + \mathbf{Z}_1, \mathbf{X} + \mathbf{Z}_2)$ Wyner-Ziv coding scheme of Section 5.1 where the source to be compressed at the relay is $\mathbf{X}_S + \mathbf{Z}_R$ and the side-information at the receiver (from the previous block) is $\mathbf{X}_S + \mathbf{Z}_D$.

The compressed $\mathbf{Y}_R(b-1)$ may now be expressed as

$$\begin{aligned}\widehat{\mathbf{Y}}_R(b-1) &= (\alpha_1^2 - \alpha_1^2\alpha_2 + \alpha_2)\mathbf{X}_S(w_{b-1}) + \alpha_2(1 - \alpha_1^2)\mathbf{Z}_D + \alpha_1^2\mathbf{Z}_R - \alpha_1\mathbf{E}_q(b-1) \\ &= \mathbf{X}_S(w_{b-1}) + \mathbf{Z}_R(b-1) - \mathbf{E}_q(b-1)\end{aligned}$$

where $\mathbf{E}_q(b-1) := (\mathbf{Y}_D(b-1) + \mathbf{U}_q(b-1)) \bmod \Lambda_q$ (with $\mathbf{U}_q(b-1)$ the quantization dither which is uniformly distributed over \mathcal{V}_q) is independent and uniformly distributed over \mathcal{V}_q with second moment D . The destination may decode $\mathbf{t}_1(w_{b-1})$ from $\mathbf{Y}'_D(b-1)$ and $\widehat{\mathbf{Y}}_R(b-1)$ by coherently combining them as

$$\begin{aligned}& \frac{\sqrt{P}}{N_D}\mathbf{Y}'_D(b-1) + \frac{\sqrt{P}}{N_R + D}\widehat{\mathbf{Y}}_R(b-1) \\ &= \left(\frac{\sqrt{P}}{N_D} + \frac{\sqrt{P}}{N_R + D} \right) \mathbf{X}_S(w_{b-1}) + \frac{\sqrt{P}}{N_D}\mathbf{Z}_D(b-1) + \frac{\sqrt{P}}{N_R + D}(\mathbf{Z}_R(b-1) - \mathbf{E}_q(b-1)). \quad (5.5)\end{aligned}$$

Now we wish to decode w_{b-1} from (Equation 5.5) which is the sum of the desired codeword which is uniformly distributed over a Rogers good lattice, and noise composed of Gaussian noise

and \mathbf{E}_q uniformly distributed over a fundamental Voronoi region of a Rogers good lattice. This scenario may be handled by Lemma 6, and we may thus uniquely decode w_{b-1} as long as

$$R < \frac{1}{2} \log \left(1 + \frac{P}{N_D} + \frac{P}{N_R + D} \right).$$

Combining this with the constraint (Equation 5.4), we obtain

$$R < \frac{1}{2} \log \left(1 + \frac{P}{N_D} + \frac{PP_R}{PN_R + PN_D + P_R N_R + N_R N_D} \right),$$

which is the CF rate achieved by the usual choice of Gaussian random codes (in which the relay quantizes the received signal \mathbf{Y}_R as $\hat{\mathbf{Y}}_R = \mathbf{Y}_R + \mathbf{E}_q$ in which \mathbf{E}_q is independent of \mathbf{Y}_R) (11, pg. 17–48).

CHAPTER 6

LATTICE CODING FOR TWO-WAY TWO-RELAY CHANNEL

The Two-way Two-relay Channel $1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4$ is a generalization of the Two-way Relay channel $1 \leftrightarrow 2 \leftrightarrow 3$ to multiple relays, where Node 1 and 4 simultaneously communicate with each other through two relay nodes 2 and 3. Each node only communicates with its neighboring nodes. As lattice codes proved useful in the Two-way Relay channel in decoding the sum at the relay, it is natural to expect lattice codes to again perform well for the considered channel. We propose, for the first time, a lattice based scheme for this two-way line network, where all nodes transmit lattice codewords and each relay node decodes a sum of these codewords. This scheme may be seen as a generalization of the lattice based scheme of (3; 2) for the Two-way Relay Channel. However, this generalization is not straightforward due to the presence of multiple relays and hence the need to repeatedly be able to decode the sum of codewords. One way to enable this is to have the relays employ lattice codewords as well – something not required in the Two-way Relay channel. In the Two-way Relay channel achievability schemes consists of two phases – the multiple access and the broadcast phase. The scheme includes multiple Block Markov phases, where during each phase, the end users send new messages encoded by lattice codewords and the relays decode a combination of lattice codewords. The relays then perform a “Re-distribution Transform” on the decoded lattice codeword combinations, and broadcasts the resulting lattice codewords. The novelty of our scheme lies in this “Re-distribution Transform” which enables the messages traveling in both directions to fully utilize

the relay transmit power. Furthermore, all decoders are lattice decoders (more computationally efficient than joint typicality decoders) and only a single nested lattice codebook pair is needed.

We first outline a simple but specially constructed nested lattice codes needed in our scheme and technical lemmas in Section 6.1. We outline the channel model in Section 6.2. We then describe a lattice based strategy for the broadcast phase of the Two-way (single) Relay channel with asymmetric uplinks in Section 6.3, which includes the key technical novelty – the “Redistribution Transform” which allows relays to intuitively spread the signals traveling in both directions to utilize the relay’s entire transmit power. We present the main achievable rate regions for the Two-way Two-relay channel in Section 6.4 before outlining extensions to half-duplex nodes and more than two relays in Section 6.5.

6.1 Simple but Special Lattice Codes for the Two-way Two-relay Channel

6.1.1 Construction

We consider a simple but specially constructed lattice codes designed for our scheme in Two-way Two-relay Channel. Consider two lattices Λ and Λ_c such that $\Lambda \subseteq \Lambda_c$ with fundamental regions $\mathcal{V}, \mathcal{V}_c$ of volumes V, V_c respectively. Here Λ is termed the *coarse* lattice which is a sublattice of Λ_c , the *fine* lattice, and hence $V \geq V_c$. When transmitting over the AWGN channel, one may use the set $\mathcal{C}_{\Lambda_c, \mathcal{V}} = \{\Lambda_c \cap \mathcal{V}(\Lambda)\}$ as the codebook. The coding rate R of this *nested* (Λ, Λ_c) *lattice pair* is defined as

$$R = \frac{1}{n} \log |\mathcal{C}_{\Lambda_c, \mathcal{V}}| = \frac{1}{n} \log \frac{V}{V_c}.$$

Nested lattice pairs were shown to be capacity achieving for the AWGN channel (25).

In this work, we only need one “good” nested lattice pair $\Lambda \subseteq \Lambda_c$, in which Λ is both Rogers good and Poltyrev good and Λ_c is Poltyrev good (see definitions of these in (65)). This lattice pair is used throughout this section. The existence of such a pair of nested lattices may be guaranteed by (25); we now describe the construction procedure of such a good nested lattice pair. Suppose the coarse lattice $\Lambda = \mathbf{B}\mathbb{Z}^n$ is both Rogers good and Poltyrev good with second moment $\sigma^2(\Lambda) = 1$. With respect to this coarse lattice Λ , the fine lattice Λ_c is generated by Construction A (25; 1), which maps a codebook of a linear block code over a finite field into real lattice points. The generation procedure is:

- Consider the vector $\mathbf{G} \in \mathbb{F}_{P_{prime}}^n$ with every element drawn from an i.i.d. uniform distribution from the finite field of order P_{prime} (a prime number) which we take to be $\mathbb{F}_{P_{prime}} = \{0, 1, 2, \dots, P_{prime} - 1\}$ under addition and multiplication modulo P_{prime} .
- The codebook $\bar{\mathcal{C}}$ of the linear block code induced by \mathbf{G} is $\bar{\mathcal{C}} = \{\bar{c} = \mathbf{G}w : w \in \mathbb{F}_{P_{prime}}\}$.
- Embed this codebook into the unit cube by scaling down by a factor of P_{prime} and then place a copy at every integer vector: $\bar{\Lambda}_c = P_{prime}^{-1} \bar{\mathcal{C}} + \mathbb{Z}^n$.
- Rotate $\bar{\Lambda}_c$ by the generator matrix of the coarse lattice to obtain the desired fine lattice: $\Lambda_c = \mathbf{B} \bar{\Lambda}_c$.

Now let $\phi(\cdot)$ denote the one-to-one mapping between one element in the one dimensional finite field $w \in \mathbb{F}_{P_{prime}}$ to a point in n -dimension real space $\mathbf{t} \in \mathcal{C}_{\Lambda_c, \nu}$:

$$\mathbf{t} = \phi(w) = (\mathbf{B} P_{prime}^{-1} \mathbf{G} w) \mod \Lambda, \quad (6.1)$$

with inverse mapping $w = \phi^{-1}(\mathbf{t}) = (\mathbf{G}^T \mathbf{G})^{-1} \mathbf{G}^T (P_{prime}(\mathbf{B}^{-1} \mathbf{t} \bmod \mathbb{Z}^n))$ (see (1, Lemma 5 and 6)). The mapping operation $\phi(\cdot)$ defined here is used in the following lemmas.

6.1.2 Technical lemmas

We first state several lemmas needed in the proposed two-way lattice based scheme. In the following, \mathbf{t}_{ai} and $\mathbf{t}_{bi} \in \mathcal{C}_{\Lambda_c, \mathcal{V}}$ are generated from w_{ai} and $w_{bi} \in \mathbb{F}_{P_{prime}}$ as $\mathbf{t}_{ai} = \phi(w_{ai})$, $\mathbf{t}_{bi} = \phi(w_{bi})$. Furthermore, let $\alpha, \alpha_i, \beta_i \in \mathbb{Z}$ such that $\frac{\alpha}{P_{prime}}, \frac{\alpha_i}{P_{prime}}, \frac{\beta_i}{P_{prime}} \notin \mathbb{Z}$ and $\theta \in \mathbb{R}$. We use \oplus , \otimes and \ominus to denote modulo P_{prime} addition, multiplication, and subtraction over the finite field $\mathbb{F}_{P_{prime}}$.

Lemma 14 *There exists an one-to-one mapping between $\mathbf{v} = (\sum_i \alpha_i \theta \mathbf{t}_{ai} + \sum_i \beta_i \theta \mathbf{t}_{bi}) \bmod \theta \Lambda$ and $\mathbf{u} = \bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi}$.*

Proof: The proof follows from (1, Lemma 6), where it is shown that there is an one-to-one mapping between $\theta^{-1} \mathbf{v} = (\sum_i \alpha_i \mathbf{t}_{ai} + \sum_i \beta_i \mathbf{t}_{bi}) \bmod \Lambda$ and $\mathbf{u}' = \bigoplus_i \alpha'_i w_{ai} \oplus \bigoplus_i \beta'_i w_{bi}$, where $\alpha'_i = \alpha_i \bmod P_{prime}$ and $\beta'_i = \beta_i \bmod P_{prime}$. This one-to-one mapping is given by $\theta^{-1} \mathbf{v} = \phi^{-1}(\mathbf{u}')$ and $\mathbf{u}' = \phi(\theta^{-1} \mathbf{v})$. Then observe that $\bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi} = \bigoplus_i \alpha'_i w_{ai} \oplus \bigoplus_i \beta'_i w_{bi}$ by the properties of modulo addition and multiplication. Thus, the one-to-one mapping between \mathbf{v} and \mathbf{u} is given by $\mathbf{v} = \theta \phi^{-1}(\mathbf{u})$ and $\mathbf{u} = \phi(\theta^{-1} \mathbf{v})$.

Lemma 15 *There exists an one-to-one mapping between $\alpha \otimes w$ and w .*

Proof: Recall that $\frac{\alpha}{P_{prime}} \notin \mathbb{Z}$. Suppose $\alpha \otimes w_1 = \alpha \otimes w_2$. Then $\alpha(w_1 - w_2) = \kappa P_{prime}$ for some integer κ . Re-writing this, we have $\frac{\alpha}{P_{prime}}(w_1 - w_2) = \kappa$ for some integer κ . This implies

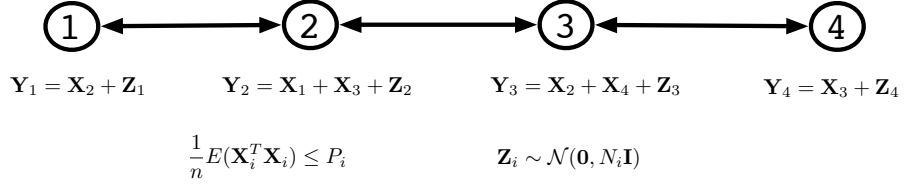


Figure 14. The Gaussian Two-way Two-relay Channel Model.

that either $\frac{\alpha}{P_{\text{prime}}} \in \mathbb{Z}$ or $\frac{w_1 - w_2}{P_{\text{prime}}} \in \mathbb{Z}$. Since $\frac{\alpha}{P_{\text{prime}}} \notin \mathbb{Z}$, $\frac{w_1 - w_2}{P_{\text{prime}}} \in \mathbb{Z}$. Thus $w_1 - w_2 = 0$ since $-(P_{\text{prime}} - 1) \leq w_1 - w_2 \leq P_{\text{prime}} - 1$. Hence $w_1 = w_2$.

Lemma 16 *If w_{ai} and w_{bi} are uniformly distributed over $\mathbb{F}_{P_{\text{prime}}}$, then $(\sum_i \alpha_i \theta \mathbf{t}_{ai} + \sum_i \beta_i \theta \mathbf{t}_{bi}) \bmod \theta \Lambda$ is uniformly distributed over $\{\theta \Lambda_c \cap \mathcal{V}(\theta \Lambda)\}$.*

Proof: As in the proof of Lemma 14, $(\sum_i \alpha_i \theta \mathbf{t}_{ai} + \sum_i \beta_i \theta \mathbf{t}_{bi}) \bmod \theta \Lambda = \theta((\sum_i \alpha_i \mathbf{t}_{ai} + \sum_i \beta_i \mathbf{t}_{bi}) \bmod \Lambda) = \theta \phi(\bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi})$. Since w_{ai} and w_{bi} are uniformly distributed over $\mathbb{F}_{P_{\text{prime}}}$, $\alpha_i w_{ai}$ and $\beta_i w_{bi}$ are uniformly distributed over $\mathbb{F}_{P_{\text{prime}}}$ by Lemma 15. Then, $\bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi}$ is uniformly distributed over $\mathbb{F}_{P_{\text{prime}}}$, and $\phi(\bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi})$ is uniformly distributed over $\{\Lambda_c \cap \mathcal{V}(\Lambda)\}$, and finally $\theta \phi(\bigoplus_i \alpha_i w_{ai} \oplus \bigoplus_i \beta_i w_{bi})$ is uniformly distributed over $\{\theta \Lambda_c \cap \mathcal{V}(\theta \Lambda)\}$.

6.2 Channel Model

The Gaussian Two-way Two-relay Channel describes a wireless communication scenario where two source nodes (Node 1 and 4) simultaneously communicate with each other through multiple full-duplex relays (Node 2 and 3) and multiple hops as shown in Figure 14. Each node

can only communicate with its neighboring nodes. The channel model may be expressed as (all bold symbols are n dimensional)

$$\mathbf{Y}_1 = \mathbf{X}_2 + \mathbf{Z}_1$$

$$\mathbf{Y}_2 = \mathbf{X}_1 + \mathbf{X}_3 + \mathbf{Z}_2$$

$$\mathbf{Y}_3 = \mathbf{X}_2 + \mathbf{X}_4 + \mathbf{Z}_3$$

$$\mathbf{Y}_4 = \mathbf{X}_3 + \mathbf{Z}_4$$

where \mathbf{Z}_i ($i \in \{1, 2, 3, 4\}$) is an i.i.d. Gaussian noise vector with variance N_i : $\mathbf{Z}_i \sim \mathcal{N}(\mathbf{0}, N_i \mathbf{I})$, and the input \mathbf{X}_i is subject to the transmit power constraint P_i : $\frac{1}{n} E(\mathbf{X}_i^T \mathbf{X}_i) \leq P_i$. Note that since we can always subtract the signal transmitted by the node itself, they are omitted in the channel model expression. Also note the arbitrary power constraints and noise variances but unit channel gains.

An $(2^{nR_a}, 2^{nR_b}, n)$ code for the Gaussian Two-way Two-relay channel consists of the two sets of messages w_a, w_b uniformly distributed over $\mathcal{M}_a := \{1, 2, \dots, 2^{nR_a}\}$ and $\mathcal{M}_b := \{1, 2, \dots, 2^{nR_b}\}$ respectively, and two encoding functions $X_1^n : \mathcal{M}_a \rightarrow \mathbb{R}^n$ (shortened to \mathbf{X}_1) and $X_4^n : \mathcal{M}_b \rightarrow \mathbb{R}^n$ (shortened to \mathbf{X}_4), satisfying the power constraints P_1 and P_4 respectively, two sets of relay functions $\{f_{k,j}\}_{j=1}^n$ ($k = 2, 3$) such that the relay channel input at time j is a function of the previously received relay channel outputs from channel uses 1 to $j - 1$, $X_{k,j} = f_{k,j}(Y_{k,1}, \dots, Y_{k,j-1})$, and finally two decoding functions $g_1 : \mathcal{Y}_1^n \times \mathcal{M}_a \rightarrow \mathcal{M}_b$ and $g_4 : \mathcal{Y}_4^n \times \mathcal{M}_b \rightarrow \mathcal{M}_a$ which yield the message estimates $\hat{w}_b := g_1(Y_1^n, w_a)$ and

$\hat{w}_a := g_2(Y_4^n, w_b)$ respectively. We define the average probability of error of the code to be $P_{n,e} := \frac{1}{2^{n(R_a+R_b)}} \sum_{w_a \in \mathcal{M}_a, w_b \in \mathcal{M}_b} \Pr\{(\hat{w}_a, \hat{w}_b) \neq (w_a, w_b) | (w_a, w_b) \text{ sent}\}$. The rate pair (R_a, R_b) is then said to be achievable by the two-relay channel if, for any $\epsilon > 0$ and for sufficiently large n , there exists an $(2^{nR_a}, 2^{nR_b}, n)$ code such that $P_{n,e} < \epsilon$. The capacity region of the Gaussian Two-way Two-relay channel is the supremum of the set of achievable rate pairs.

6.3 Lattice Codes in the BC Phase of the Two-way Relay Channel

The work (3; 2) introduces a two-phase lattice scheme for the Gaussian Two-way Relay Channel $1 \leftrightarrow 2 \leftrightarrow 3$, where two user nodes 1 and 3 exchange information through a single relay node 2 (all definitions are analogous to the previous section): the Multiple-access Channel (MAC) phase and the Broadcast Channel (BC) phase. In the MAC phase, the relay receives a noisy version of the sum of two signals from both users as in a multiple access channel (MAC). If the codewords are from nested lattice codebooks, the relay may decode the sum of the two codewords directly without decoding them individually. This is sufficient for this channel, as then, in the BC phase, the relay may broadcast the sum of the codewords to both users who may determine the other message using knowledge of their own transmitted message. In the scheme of (3), the relay re-encodes the decoded sum of the codewords into a codeword from an i.i.d. random codebook while (2) uses a lattice codebook in the downlink.

In extending the schemes of (3; 2) to multiple relays we would want to use lattice codebooks in the BC phase, as in (2). This would, for example, allow the signal sent by Node 2 to be aligned with Node 4's transmitted signal (aligned is used to mean that the two codebooks are nested) in the Two-way Two-relay Channel: $1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4$ and hence enable the decoding

of the sum of codewords again at Node 3. However, the scheme of (2) is only applicable to channels in which the SNR from the users to the relay are symmetric, i.e. $\frac{P_1}{N_2} = \frac{P_3}{N_2}$. In this case the relay can simply broadcast the decoded (and possibly scaled) sum of codewords sum without re-encoding it. Thus, before tackling the Two-way Two-relay channel, we first devise a lattice-coding scheme for the BC phase in the Two-way Relay Channel with *arbitrary* uplink SNRs $\frac{P_1}{N_2} \neq \frac{P_3}{N_2}$.

In this section, we design a lattice coding scheme for the BC phase of the Gaussian Two-way (single-relay) Channel with arbitrary uplink SNR – i.e. not restricted to symmetric SNRs as in (2). A similar technique will be utilized in the lattice coding scheme for Two-way Two-relay Channel in Section 6.4.

The channel model is the same as in (3): two users Node 1 and 3 communicate with each other through the relay Node 2. The channel model is expressed as

$$\mathbf{Y}_1 = \mathbf{X}_2 + \mathbf{Z}_1$$

$$\mathbf{Y}_2 = \mathbf{X}_1 + \mathbf{X}_3 + \mathbf{Z}_2$$

$$\mathbf{Y}_3 = \mathbf{X}_2 + \mathbf{Z}_3$$

where \mathbf{Z}_i ($i \in \{1, 2, 3\}$) is an i.i.d. Gaussian noise vector with variance N_i : $\mathbf{Z}_i \sim \mathcal{N}(\mathbf{0}, N_i \mathbf{I})$, and the input \mathbf{X}_i is subject to the transmitting power constraint P_i : $\frac{1}{n} E(\mathbf{X}_i^T \mathbf{X}_i) \leq P_i$. Similar definitions of codes and achievability as in Section 6.2 are assumed.

We will devise an achievability scheme which uses lattice codes in both the MAC phase and BC phase. For simplicity, to demonstrate the central idea of a lattice-based BC phase which is going to be used in the Two-way Two-relay Channel, we do not use dithers nor MMSE scaling as in (25; 3; 2)¹.

We assume that $P_1 = N^2 p^2$ and $P_3 = p^2$ where $p \in \mathbb{R}$ and $N \in \mathbb{Z}$. This assumption will be generalized to arbitrary power constraints in the next section. We focus on the symmetric rate for the Two-way Two-relay Channel, i.e. when the coding rates of the two messages are identical.

Codebook generation: Consider the messages $w_a, w_b \in \mathbb{F}_{P_{prime}} = \{0, 1, 2, \dots, P_{prime} - 1\}$. P_{prime} is a large prime number such that $P_{prime} = \lceil 2^{nR_{sym}} \rceil$, where R_{sym} is the symmetric coding rate and $\lceil \cdot \rceil$ denotes rounding to the nearest prime ($P_{prime} = \lceil 2^{nR_{sym}} \rceil \rightarrow \infty$ as $n \rightarrow \infty$ since there are infinitely many primes). The two users Node 1 and 2 send the codewords $\mathbf{X}_1 = Np\mathbf{t}_a = Np\phi(w_a)$ and $\mathbf{X}_2 = p\mathbf{t}_b = p\phi(w_b)$ where $\phi(\cdot)$ is defined in (Equation 6.1) in Section 6.1.1 with the nested lattices $\Lambda \subseteq \Lambda_c$. Notice that their codebooks are scaled versions of the codebook $\mathcal{C}_{\Lambda_c, \nu}$. The symmetric coding rate is then $R_{sym} := \frac{1}{n} \log \frac{V(\Lambda)}{V(\Lambda_c)}$.

¹Dithers and MMSE scaling allows one to go from achieving rates proportional to $\log(SNR)$ to $\log(1 + SNR)$. However, we initially forgo the “1+” term for simplicity and so as not to clutter the main idea with additional dithers and MMSE scaling.

In the MAC phase, the relay receives $\mathbf{Y}_2 = \mathbf{X}_1 + \mathbf{X}_3 + \mathbf{Z}_2$ and decodes $(Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda$ with arbitrarily low probability of error as $n \rightarrow \infty$ with rate constraints

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_1}{N_2} \right) \right]^+$$

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_3}{N_2} \right) \right]^+$$

according to Lemma 17.

Lemma 17 *Let $\mathbf{X}_a = \alpha\theta\mathbf{t}_a = \alpha\theta\phi(w_a) \in \{\alpha\theta\Lambda_c \cap \mathcal{V}(\alpha\theta\Lambda)\}$ and $\mathbf{X}_b = \theta\mathbf{t}_b = \theta\phi(w_b) \in \{\theta\Lambda_c \cap \mathcal{V}(\theta\Lambda)\}$ where $w_a, w_b \in \mathbb{F}_{P_{prime}}$, $\alpha \in \mathbb{Z}^+$, $\theta \in \mathbb{R}^+$ and $\phi(\cdot), \Lambda \subseteq \Lambda_c$ are defined as in Section 6.1.1 with $R := \frac{1}{n} \log \frac{V(\Lambda)}{V(\Lambda_c)}$. From the received signal $\mathbf{Y} = \mathbf{X}_a + \mathbf{X}_b + \mathbf{Z}$ where $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_z^2 \mathbf{I})$ one may decode $(\alpha\theta\mathbf{t}_a + \theta\mathbf{t}_b) \bmod \alpha\theta\Lambda$ with arbitrary low probability of error as $n \rightarrow \infty$ at rates*

$$R < \left[\frac{1}{2} \log \frac{\sigma^2(\alpha\theta\Lambda)}{\sigma_z^2} \right]^+$$

$$R < \left[\frac{1}{2} \log \frac{\sigma^2(\theta\Lambda)}{\sigma_z^2} \right]^+.$$

Proof: The proof generally follows (3), except that for simplicity, we do not use dithers or MMSE scaling of the received signal in our scheme. The receiver processes the received signal as

$$\begin{aligned}\mathbf{Y} \bmod \alpha\theta\Lambda &= \mathbf{X}_a + \mathbf{X}_b + \mathbf{Z} \bmod \alpha\theta\Lambda \\ &= \alpha\theta\mathbf{t}_a + \theta\mathbf{t}_b + \mathbf{Z} \bmod \alpha\theta\Lambda\end{aligned}$$

To decode $(\alpha\theta\mathbf{t}_a + \theta\mathbf{t}_b) \bmod \alpha\theta\Lambda$, the effective noise is given by \mathbf{Z} with variance σ_z^2 rather than the equivalent noise after MMSE scaling as in (3). All other steps remain identical. The effective signal-to-noise ratios are $SNR_a = \frac{\sigma^2(\alpha\theta\Lambda_a)}{\sigma_z^2}$ and $SNR_b = \frac{\sigma^2(\theta\Lambda_b)}{\sigma_z^2}$, resulting in the given rate constraints.

In the BC phase, if, mimicking the steps of (2) the relay simply broadcasts the scaled version of $(Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda$

$$\frac{\sqrt{P_2}}{Np}((Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda) = \left(\sqrt{P_2}\mathbf{t}_a + \frac{\sqrt{P_2}}{N}\mathbf{t}_b \right) \bmod \sqrt{P_2}\Lambda,$$

we would achieve the rate $R_{sym} < [\frac{1}{2} \log \frac{P_2}{N_3}]^+$ for the direction $2 \rightarrow 3$ and the rate $R_{sym} < [\frac{1}{2} \log \frac{P_2}{NN_1}]^+$ for the $1 \leftarrow 2$ direction. While the rate constraint for the direction $2 \rightarrow 3$ is as large as expected, the rate constraint for the direction $1 \leftarrow 2$ does not fully utilize the power at the relay, i.e. the codeword \mathbf{t}_b appears to use only the power P_2/N rather than the full power P_2 . One would thus want to somehow transform the decoded sum $(Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda$ such that both \mathbf{t}_a and \mathbf{t}_b of the transformed signal would be uniformly distributed over $\mathcal{V}(\sqrt{P_2}\Lambda)$.

Notice that the relay can only operate on $(Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda$ rather than $Np\mathbf{t}_a$ and $p\mathbf{t}_b$ individually.

Re-distribution Transform: To alleviate this problem we propose the following “Re-distribution Transform” operation which consists of three steps:

1. multiply the decoded signal by N to obtain $N((Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda)$,
2. then take $\bmod \Lambda$ to obtain

$$N((Np\mathbf{t}_a + p\mathbf{t}_b) \bmod Np\Lambda) \bmod \Lambda = (N^2p\mathbf{t}_a + Np\mathbf{t}_b) \bmod Np\Lambda$$

according to the operation rule in (Equation 3.1), and finally

3. re-scale the signal to be of second moment P_2 as

$$\frac{\sqrt{P_2}}{Np}((N^2p\mathbf{t}_a + Np\mathbf{t}_b) \bmod Np\Lambda) = (N\sqrt{P_2}\mathbf{t}_a + \sqrt{P_2}\mathbf{t}_b) \bmod \sqrt{P_2}\Lambda$$

according to the operation rule in (Equation 3.2). Notice that $(N\sqrt{P_2}\mathbf{t}_a + \sqrt{P_2}\mathbf{t}_b) \bmod \sqrt{P_2}\Lambda$ is uniformly distributed over $\{\sqrt{P_2}\Lambda_c \cap \mathcal{V}(\sqrt{P_2}\Lambda)\}$ by Lemma 16.

The three steps of the Re-distribution Transform procedure are illustrated in Figure 15 for a simple one-dimensional lattice in order to gain some intuition and insight (though we operate in n -dimensions in our achievability proof). In this simple example, Node 1 sends $2p\mathbf{t}_a \in \{2p\Lambda_c \cap$

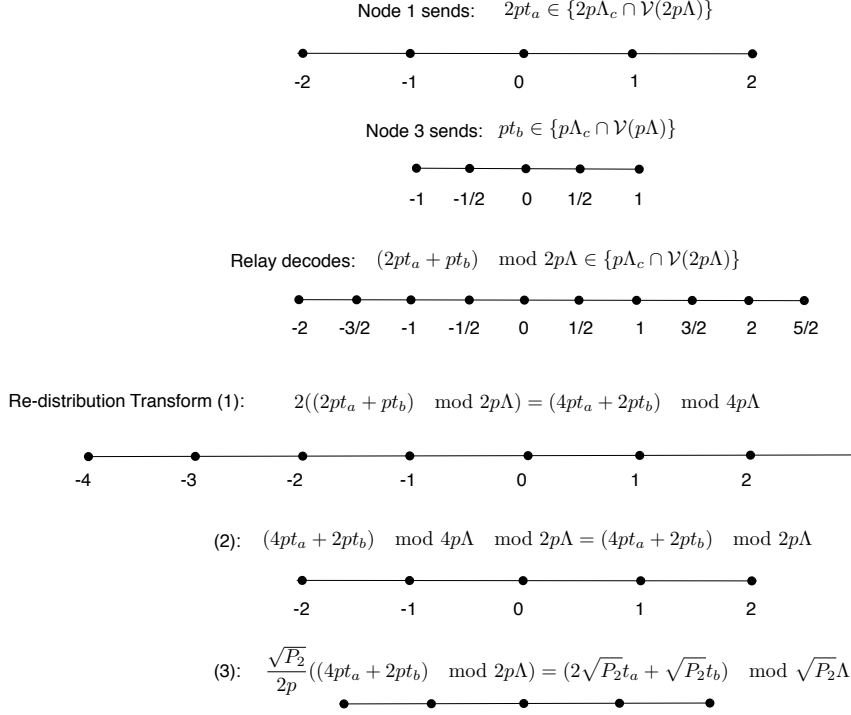


Figure 15. Re-distribution Transform illustration for a one-dimensional lattice.

$\mathcal{V}(2p\Lambda)\} = \{-2, -1, 0, 1, 2\}$ and Node 3 sends $pt_b \in \{p\Lambda_c \cap \mathcal{V}(p\Lambda)\} = \{-1, -1/2, 0, 1/2, 1\}$. The relay decodes

$$(2pt_a + pt_b) \bmod 2p\Lambda \in \{p\Lambda_c \cap \mathcal{V}(2p\Lambda)\} = \{-2, -3/2, -1, -1/2, 0, 1/2, 1, 3/2, 2, 5/2\}$$

and transforms it into $(4pt_a + 2pt_b) \bmod 2p\Lambda \in \{2p\Lambda_c \cap \mathcal{V}(2p\Lambda)\} = \{-2, -1, 0, 1, 2\}$ according to the three steps in the Re-distribution Transform. Notice $|\{2p\Lambda_c \cap \mathcal{V}(2p\Lambda)\}| < |\{p\Lambda_c \cap \mathcal{V}(2p\Lambda)\}|$, and hence the transformed signal is thus easier to forward.

The relay broadcasts $\mathbf{X}_2 = (N\sqrt{P_2}\mathbf{t}_a + \sqrt{P_2}\mathbf{t}_b) \bmod \sqrt{P_2}\Lambda$. Notice that $(N\sqrt{P_2}\mathbf{t}_a + \sqrt{P_2}\mathbf{t}_b) \bmod \sqrt{P_2}\Lambda$ is uniformly distributed over $\{\sqrt{P_2}\Lambda_c \cap \mathcal{V}(\sqrt{P_2}\Lambda)\}$, and so its coding rate is R_{sym} . Node 1 and Node 3 receive $\mathbf{Y}_1 = \mathbf{X}_2 + \mathbf{Z}_1$ and $\mathbf{Y}_3 = \mathbf{X}_2 + \mathbf{Z}_3$ respectively and, according to Lemma 18, may decode $(N\sqrt{P_2}\mathbf{t}_a + \sqrt{P_2}\mathbf{t}_b) \bmod \sqrt{P_2}\Lambda$ at rate

$$R_{sym} < \left[\frac{1}{2} \log \frac{P_2}{N_1} \right]^+ \\ R_{sym} < \left[\frac{1}{2} \log \frac{P_2}{N_3} \right]^+.$$

Lemma 18 *Let $\mathbf{X} = \theta\mathbf{t} = \theta\phi(w) \in \{\theta\Lambda_c \cap \mathcal{V}(\theta\Lambda)\}$ where $\theta \in \mathbb{R}^+$, $w \in \mathbb{F}_{P_{prime}}$ and $\phi(\cdot), \Lambda \subseteq \Lambda_c$ are defined as in Section 6.1.1, with $R = \frac{1}{n} \log \frac{V(\Lambda)}{V(\Lambda_c)}$. From the received signal $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$ where $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_z^2 \mathbf{I})$, one may decode $\theta\mathbf{t}$ with arbitrary low probability of error as $n \rightarrow \infty$ at rate*

$$R < \frac{1}{2} \log \frac{\sigma^2(\theta\Lambda)}{\sigma_z^2}.$$

Proof: The proof generally follows (25, Theorem 5), except that we do not use dithers nor MMSE scaling in our scheme. The receiver processes the received signal as

$$\begin{aligned} \mathbf{Y} \bmod \Lambda &= \mathbf{X} + \mathbf{Z} \bmod \Lambda \\ &= \mathbf{t} + \mathbf{Z} \bmod \Lambda \end{aligned}$$

To decode \mathbf{t} , the effective noise is \mathbf{Z} with variance σ_z^2 rather than an equivalent noise after MMSE as in (25, Theorem 5). All other steps are identical. The effective signal-to-noise ratio is thus $SNR = \frac{\sigma^2(\theta\Lambda)}{\sigma_z^2}$, and we obtain the rate constraints as in the lemma statement.

Nodes 1 and 2 then map the decoded $(NP_R\mathbf{t}_a + P_R\mathbf{t}_b) \bmod P_R\Lambda$ to $Nw_a \oplus w_b$ by Lemma 14. With side information w_a , Node 1 may then determine w_b ; likewise with side information w_b , Node 2 can obtain Nw_a and then determine w_a by Lemma 15.

6.4 The proposed protocol and achievable rates for the Two-way Two-relay channel

We first consider the full-duplex Two-way Two-relay channel where every node transmits and receives at the same time. For this channel model we first obtain an achievable rate region for special relationships between the power constraints at the four nodes in Theorem 19, and the related Lemma 20. We then use these results to obtain an achievable rate region for the general (arbitrary powers) Gaussian Two-way Two-relay channel, which we show is to within $\frac{1}{2} \log(3)$ bits/s/Hz per user of the symmetric rate capacity in Theorem 21.

Theorem 19 *For the channel model described in Section 6.2, if $P_1 = p^2$, $P_2 = M^2q^2$, $P_3 = N^2p^2$ and $P_4 = q^2$, where $p, q \in \mathbb{R}^+$ and $M, N \in \mathbb{Z}^+$ the following rate region*

$$R_a, R_b < \min \left(\left[\frac{1}{2} \log \left(\frac{P_1}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_2}{N_3} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_3}{N_4} \right) \right]^+, \right. \\ \left. \left[\frac{1}{2} \log \left(\frac{P_4}{N_3} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_3}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_2}{N_1} \right) \right]^+ \right) \quad (6.2)$$

is achievable using lattice codes.

Proof: *Codebook generation:* We consider the good nested lattice pair $\Lambda \subseteq \Lambda_c$ with corresponding codebook $\mathcal{C}_{\Lambda_c, \mathcal{V}} = \{\Lambda_c \cap \mathcal{V}(\Lambda)\}$, and two messages $w_a, w_b \in \mathbb{F}_{P_{prime}} = \{0, 1, 2, \dots, P_{prime} - 1\}$ in which P_{prime} is a large prime number such that $P_{prime} = \lceil 2^{nR_{sym}} \rceil$ (R_{sym} is the coding rate). The codewords associated with the messages w_a and w_b are $\mathbf{t}_a = \phi(w_a)$ and $\mathbf{t}_b = \phi(w_b)$, where the mapping $\phi(\cdot)$ from $\mathbb{F}_{P_{prime}}$ to $\mathcal{C}_{\Lambda_c, \mathcal{V}} \in \mathbb{R}^n$ is defined in (Equation 6.1) in Section 6.1.1.

Encoding and decoding steps: We use a Block Markov Encoding/Decoding scheme where Node 1 and 4 transmit a new message w_{ai} and w_{bi} , respectively, at the beginning of block i . To satisfy the transmit power constraints, Node 1 and 4 send the scaled codewords $\mathbf{X}_{1i} = p\mathbf{t}_{ai} = p\phi(w_{ai}) \in \{p\Lambda_c \cap \mathcal{V}(p\Lambda)\}$ and $\mathbf{X}_{4i} = q\mathbf{t}_{bi} = q\phi(w_{bi}) \in \{q\Lambda_c \cap \mathcal{V}(q\Lambda)\}$ respectively in block i . Node 2 and 3 send \mathbf{X}_{2i} and \mathbf{X}_{3i} , and Node j ($j = \{1, 2, 3, 4\}$) receives \mathbf{Y}_{ji} in block i . The procedure of the first few blocks (the initialization steps) are described and then a generalization is made. We note that in general the coding rates R_a for w_a and R_b for w_b may be different, as long as $R_{sym} = \max(R_a, R_b)$, since we may always send dummy messages to make the two coding rates equal.

Block 1: Node 1 and 4 send new codewords $\mathbf{X}_{11} = p\mathbf{t}_{a1}$ and $\mathbf{X}_{41} = q\mathbf{t}_{b1}$ to Node 2 and 3 respectively. Node 2 and 3 can decode the transmitted codeword with vanishing probability of error if

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_1}{N_2} \right) \right]^+ \quad (6.3)$$

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_4}{N_3} \right) \right]^+ \quad (6.4)$$

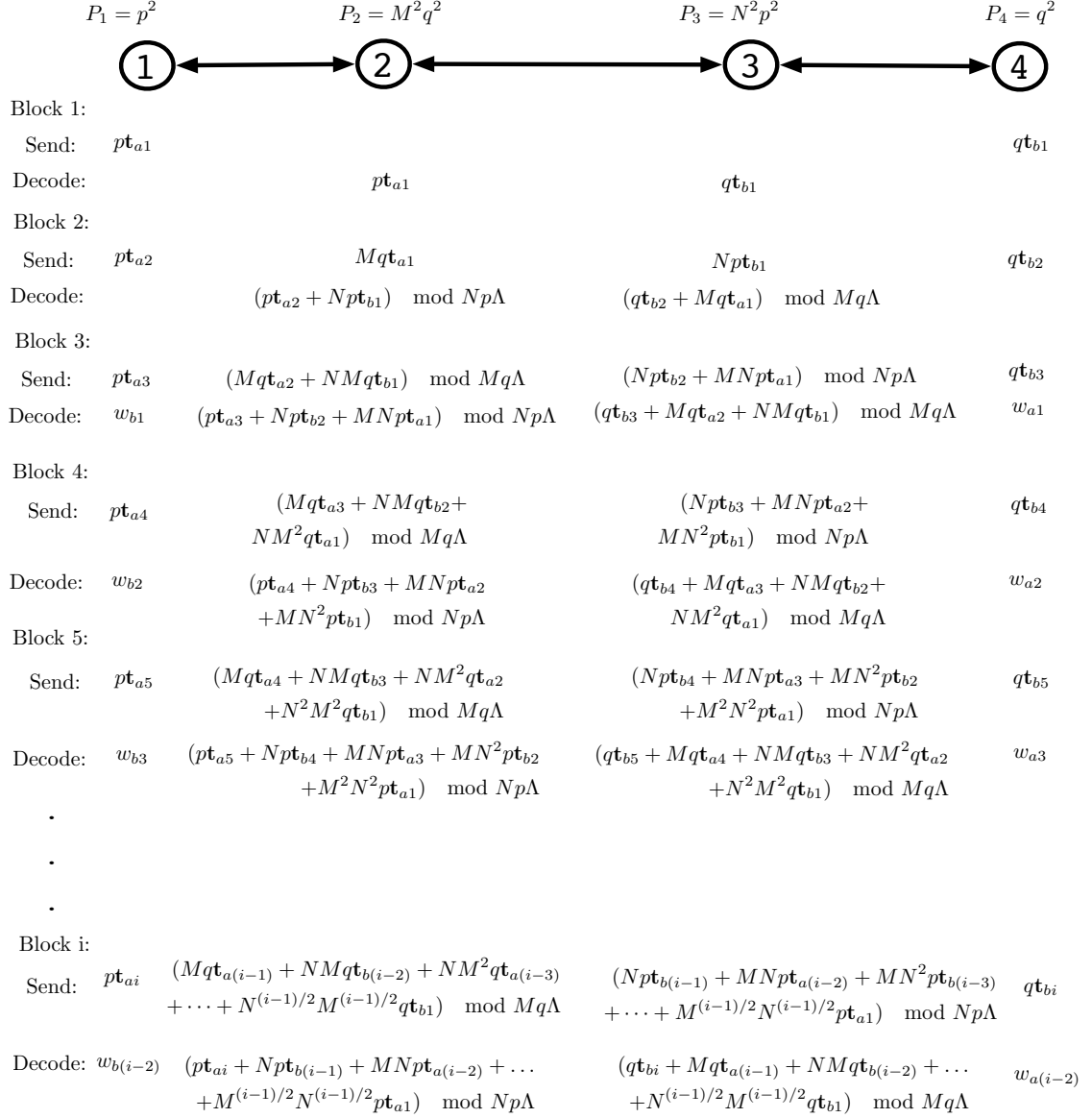


Figure 16. Multi-phase Block Markov achievability strategy for Theorem 19.

according to Lemma 18.

Block 2: Node 1 and 4 send their respective new codewords $\mathbf{X}_{12} = p\mathbf{t}_{a2}$ and $\mathbf{X}_{42} = q\mathbf{t}_{b2}$, while Node 2 and 3 broadcast $\mathbf{X}_{22} = Mq\mathbf{t}_{a1}$ and $\mathbf{X}_{32} = Np\mathbf{t}_{b1}$ received in the last block. Note they are scaled to fully utilize the transmit power $P_2 = M^2q^2$ and $P_3 = N^2p^2$. Node 2 receives $\mathbf{Y}_{22} = \mathbf{X}_{12} + \mathbf{X}_{32} + \mathbf{Z}_{22}$ and decodes $(p\mathbf{t}_{a2} + Np\mathbf{t}_{b1}) \bmod Np\Lambda$ with arbitrarily low probability of error if R satisfies (Equation 6.3) and

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_3}{N_2} \right) \right]^+. \quad (6.5)$$

Similarly, Node 3 can decode $(q\mathbf{t}_{b2} + Mq\mathbf{t}_{a1}) \bmod Mq\Lambda$ subject to (Equation 6.4) and

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_2}{N_3} \right) \right]^+. \quad (6.6)$$

Block 3:

- *Encoding:* Node 1 and 4 send new codewords as in the previous blocks. Node 2 further processes its decoded codewords combination according to the three steps of the Redistribution Transform from previous block as

$$\begin{aligned} (N((p\mathbf{t}_{a2} + Np\mathbf{t}_{b1}) \bmod Np\Lambda)) \bmod Np\Lambda &= (Np\mathbf{t}_{a2} + N^2p\mathbf{t}_{b1}) \bmod N^2p\Lambda \bmod Np\Lambda \\ &= (Np\mathbf{t}_{a2} + N^2p\mathbf{t}_{b1}) \bmod Np\Lambda \end{aligned}$$

including scaling to fully utilize the transmit power $P_2 = M^2 q^2$ as

$$\frac{Mq}{Np}(Np\mathbf{t}_{a2} + N^2p\mathbf{t}_{b1}) \mod Np\Lambda = (Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda.$$

It then broadcasts $\mathbf{X}_{23} = (Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda$. Notice that since

$$(Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda \in \{Mq\Lambda_c \cap \mathcal{V}(Mq\Lambda)\}$$

according to Lemma 16, its coding rate is R_{sym} . Similarly, Node 3 broadcasts $\mathbf{X}_{33} = (Np\mathbf{t}_{b2} + MNp\mathbf{t}_{a1}) \mod Np\Lambda$ again at coding rate R_{sym} .

- *Decoding:* At the end of this block, Node 2 is able to decode $(p\mathbf{t}_{a3} + Np\mathbf{t}_{b2} + MNp\mathbf{t}_{a1}) \mod Np\Lambda$ with rate constraints (Equation 6.3) and (Equation 6.5) according to Lemma 17, and Node 3 decodes $(q\mathbf{t}_{b3} + Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda$ with constraints (Equation 6.6) and (Equation 6.4). Node 1 decodes $(Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda$ sent by Node 2 as in the point-to-point channel with rate constraint

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_2}{N_1} \right) \right]^+ \quad (6.7)$$

according to Lemma 18. From the decoded $(Mq\mathbf{t}_{a2} + NMq\mathbf{t}_{b1}) \mod Mq\Lambda$, it obtains $w_{a2} \oplus Nw_{b1}$ (Lemma 14). With its own information w_{a2} , Node 1 can then obtain $N \otimes w_{b1} = w_{a2} \oplus Nw_{b1} \ominus w_{a2}$, which may be mapped to w_{b1} since P_{prime} is a prime number (Lemma

15). Notice $P_{prime} = \lceil 2^{nR_{sym}} \rceil \rightarrow \infty$ as $n \rightarrow \infty$, so $N \ll P_{prime} = \lceil 2^{nR} \rceil$ and $\frac{N}{P_{prime}} \notin \mathbb{Z}$.

Similarly, Node 4 can decode w_{a1} with rate constraint

$$R_{sym} < \left[\frac{1}{2} \log \left(\frac{P_2}{N_3} \right) \right]^+. \quad (6.8)$$

Block 4 and 5 proceed in a similar manner, as shown in Figure 16.

Block i : To generalize, in Block i (assume i is odd)¹,

- *Encoding*: Node 1 and 4 send new messages $\mathbf{X}_{1i} = p\mathbf{t}_{ai}$ and $\mathbf{X}_{4i} = q\mathbf{t}_{bi}$ respectively. Node 2 and 3 broadcast

$$\mathbf{X}_{2i} = (Mq\mathbf{t}_{a(i-1)} + NMq\mathbf{t}_{b(i-2)} + NM^2q\mathbf{t}_{a(i-3)} + N^2M^2q\mathbf{t}_{b(i-4)} + \cdots + N^{(i-1)/2}M^{(i-1)/2}q\mathbf{t}_{b1}) \mod Mq\Lambda$$

$$\mathbf{X}_{3i} = (Np\mathbf{t}_{b(i-1)} + MNp\mathbf{t}_{a(i-2)} + MN^2p\mathbf{t}_{b(i-3)} + M^2N^2p\mathbf{t}_{a(i-4)} + \cdots + M^{(i-1)/2}N^{(i-1)/2}p\mathbf{t}_{a1}) \mod Np\Lambda.$$

- *Decoding*: Node 1 decodes the codeword from Node 2 with rate constraint (Equation 6.7) (Lemma 18) and maps it to $w_{a(i-1)} \oplus Nw_{b(i-2)} \oplus NMw_{a(i-3)} \oplus N^2Mw_{b(i-4)} \oplus \cdots \oplus N^{(i-1)/2}M^{(i-1)/2-1}w_{b1}$ (Lemma 14). With its own messages w_{ai} ($\forall i$) and the messages it decoded previously $\{w_{b1}, w_{b2}, \dots, w_{b(i-3)}\}$, Node 1 can obtain $N \otimes w_{b(i-2)}$ and determine $w_{b(i-2)}$ accordingly (Lemma 15). Similarly, Node 4 can decode $w_{a(i-2)}$ subject to rate constraint (Equation 6.8).

¹For i even we have analogous steps with slightly different indices as may be extrapolated from the difference between Block 4 and 5 in Figure 16, which result in the same rate constraints.

- *Re-distribution Transform:* In this block i , Node 2 also decodes

$$(p\mathbf{t}_{ai} + Np\mathbf{t}_{b(i-1)} + MNp\mathbf{t}_{a(i-2)} + MN^2p\mathbf{t}_{b(i-3)} + M^2N^2p\mathbf{t}_{a(i-4)} + \dots + M^{(i-1)/2}N^{(i-1)/2}p\mathbf{t}_{a1}) \mod Np\Lambda$$

from its received signal $\mathbf{Y}_{2i} = \mathbf{X}_{1i} + \mathbf{X}_{3i} + \mathbf{Z}_{2i}$ subject to rate constraints (Equation 6.3)

and (Equation 6.5) (Lemma 17). It then uses the Re-distribution Transform to process the codeword combination as

$$\begin{aligned} & (N(p\mathbf{t}_{ai} + Np\mathbf{t}_{b(i-1)} + MNp\mathbf{t}_{a(i-2)} + \dots + M^{(i-1)/2}N^{(i-1)/2}p\mathbf{t}_{a1}) \mod Np\Lambda) \mod Np\Lambda \\ &= (Np\mathbf{t}_{ai} + N^2p\mathbf{t}_{b(i-1)} + MN^2p\mathbf{t}_{a(i-2)} + \dots + M^{(i-1)/2}N^{(i-1)/2+1}p\mathbf{t}_{a1}) \mod N^2p\Lambda \mod Np\Lambda \\ &= Np\mathbf{t}_{ai} + N^2p\mathbf{t}_{b(i-1)} + MN^2p\mathbf{t}_{a(i-2)} + \dots + M^{(i-1)/2}N^{(i-1)/2+1}p\mathbf{t}_{a1} \mod Np\Lambda \end{aligned}$$

and scales it to fully utilize the transmit power:

$$\begin{aligned} & \frac{Mq}{Np} (Np\mathbf{t}_{ai} + N^2p\mathbf{t}_{b(i-1)} + MN^2p\mathbf{t}_{a(i-2)} + \dots + M^{(i-1)/2}N^{(i-1)/2+1}p\mathbf{t}_{a1}) \mod Np\Lambda \\ &= Mq\mathbf{t}_{ai} + NMq\mathbf{t}_{b(i-1)} + NM^2q\mathbf{t}_{a(i-2)} + \dots + N^{(i-1)/2}M^{(i-1)/2+1}q\mathbf{t}_{a1} \mod Mq\Lambda. \end{aligned}$$

This signal will be transmitted in the next block $i + 1$. Node 3 performs similar operations, decoding $q\mathbf{t}_{bi} + Mq\mathbf{t}_{a(i-1)} + NMq\mathbf{t}_{b(i-2)} + \dots + N^{(i-1)/2}M^{(i-1)/2}q\mathbf{t}_{b1} \mod Mq\Lambda$ subject to constraints (Equation 6.6) and (Equation 6.4), and transforms it into $Np\mathbf{t}_{bi} + MNp\mathbf{t}_{a(i-1)} + MN^2p\mathbf{t}_{b(i-2)} + \dots + M^{(i-1)/2}N^{(i-1)/2+1}p\mathbf{t}_{b1} \mod Mq\Lambda$, which is transmitted in the next block.

Combining all rate constraints, we obtain

$$R_{sym} < \min \left(\left[\frac{1}{2} \log \left(\frac{P_1}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_2}{N_3} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_3}{N_4} \right) \right]^+, \right. \\ \left. \left[\frac{1}{2} \log \left(\frac{P_4}{N_3} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_3}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P_2}{N_1} \right) \right]^+ \right)$$

Assuming there are I blocks in total, the final achievable rate is $\frac{I-2}{I}R_{sym}$, which, as $I \rightarrow \infty$, approaches R_{sym} and we obtain (Equation 6.2).

In the above we had assumed power constraints of the form $P_1 = p^2$, $P_2 = M^2q^2$, $P_3 = N^2p^2$ and $P_4 = q^2$, where $p, q \in \mathbb{R}^+$ and $M, N \in \mathbb{Z}^+$. Analogously, we may permute some of these power constraints to achieve the same region as follows:

Lemma 20 *The rates achieved in Theorem 19 may also be achieved when $P_1 = N^2p^2$, $P_3 = p^2$ and/or $P_2 = q^2$, $P_4 = M^2q^2$.*

Proof: The proof follows the same lines as that of Theorem 19, and consists of the steps outlined in in Figure 19 in Appendix .3. In particular, since the nodes have different power constraints the scaling of the codewords is different. However, as in the previous Theorem, we only need \mathbf{X}_1 and \mathbf{X}_3 to be aligned (nested codebooks), and \mathbf{X}_2 and \mathbf{X}_4 to be aligned. As in Theorem 19, the relay nodes again decode the sum of codewords, perform the Re-distribution Transform, with a new power scaling to fully utilize their transmit power, and broadcast the re-distributed sum of codewords.

Theorem 19 and Lemma 20 both hold for powers for which P_1/P_3 and/or P_2/P_4 are either the squares of integers or the reciprocal of the squares of integers. However, these scenarios do

not cover general power constraints with arbitrary ratios. We next present an achievable rate region for arbitrary powers, obtained by appropriately clipping the power of the nodes such that the new, lower powers are indeed either the squares or the reciprocals of the squares of integers. We then show that this clipping of the power at the nodes does not result in more than a $\frac{1}{2} \log(3)$ bits/s/Hz loss in the symmetric rate.

Theorem 21 *For the Two-way Two-relay Channel with arbitrary transmit power constraints, any rates satisfying*

$$R_a, R_b < R_{achievable} = \max_{P'_i \leq P_i, \frac{P'_1}{P'_3} = N^2 \text{ or } \frac{1}{N^2}, \frac{P'_2}{P'_4} = M^2 \text{ or } \frac{1}{M^2}} \min \left(\left[\frac{1}{2} \log \left(\frac{P'_1}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_2}{N_3} \right) \right]^+, \right. \\ \left. \left[\frac{1}{2} \log \left(\frac{P'_3}{N_4} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_4}{N_3} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_3}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_2}{N_1} \right) \right]^+ \right) \quad (6.9)$$

for some $N, M \in \mathbb{Z}^+$ and $i \in \{1, 2, 3, 4\}$, are achievable. This rate region is within $\frac{1}{2} \log 3$ bit/Hz/s per user from the symmetric rate capacity.

Proof: Since P_1/P_3 and/or P_2/P_4 are in general neither the squares or the reciprocals of the squares of integers, we cannot directly apply Theorem 19. Instead, we first truncate the transmit powers P_i to P'_i such that P'_i satisfy either the constraints of Theorem 19 or Lemma 20. The achievable rate region then follows immediately for the reduced power constraints P'_i . For example, if $P_1 = 1$ and $P_3 = 3.6$, we may choose $P'_1 = 0.9$ and $P'_3 = 3.6$, so that $P'_3/P'_1 = 2^2$. Optimizing over the truncated or clipped powers yields the achievable rate region stated in Theorem 21.

An outer bound to the symmetric capacity of the AWGN Two-way Two-relay Channel is given by the minimum of the all the point-to-point links, i.e.

$$R_a, R_b < R_{outer} = \min \left(C \left(\frac{P_1}{N_2} \right), C \left(\frac{P_2}{N_3} \right), C \left(\frac{P_3}{N_4} \right), C \left(\frac{P_4}{N_3} \right), C \left(\frac{P_3}{N_2} \right), C \left(\frac{P_2}{N_1} \right) \right). \quad (6.10)$$

To evaluate the gap between (Equation 6.9) and (Equation 6.10):

$$R_{achievable} + \frac{1}{2} \log 3 \quad (6.11)$$

$$\stackrel{(a)}{=} \max_{P'_1 \leq P_1, P'_3 \leq P_3, \frac{P'_1}{P'_3} = N^2 \text{ or } \frac{1}{N^2}} \min \left(\left[\frac{1}{2} \log \left(\frac{P'_1}{N_2} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_3}{N_4} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_3}{N_2} \right) \right]^+ \right) + \frac{1}{2} \log 3 \quad (6.12)$$

$$= \max_{P'_1 \leq P_1, P'_3 \leq P_3, \frac{P'_1}{P'_3} = N^2 \text{ or } \frac{1}{N^2}} \max \left(\min \left(\frac{1}{2} \log \left(\frac{3P'_1}{N_2} \right), \frac{1}{2} \log \left(\frac{3P'_3}{N_4} \right), \frac{1}{2} \log \left(\frac{3P'_3}{N_2} \right) \right), \frac{1}{2} \log 3 \right) \quad (6.13)$$

$$\stackrel{(b)}{\geq} \max \left(\min \left(\frac{1}{2} \log \left(\frac{3P_1^*}{N_2} \right), \frac{1}{2} \log \left(\frac{3P_3^*}{N_4} \right), \frac{1}{2} \log \left(\frac{3P_3^*}{N_2} \right) \right), \frac{1}{2} \log 3 \right) \quad (6.14)$$

$$\stackrel{(c)}{\geq} \min \left(\frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right), \frac{1}{2} \log \left(1 + \frac{P_3}{N_4} \right), \frac{1}{2} \log \left(1 + \frac{P_3}{N_2} \right) \right) \quad (6.15)$$

$$\geq R_{outer}. \quad (6.16)$$

The first equality (a) follows from an assumption that WLOG, one of $\left[\frac{1}{2} \log \left(\frac{P'_1}{N_2} \right) \right]^+$, $\left[\frac{1}{2} \log \left(\frac{P'_3}{N_4} \right) \right]^+$, or $\left[\frac{1}{2} \log \left(\frac{P'_3}{N_2} \right) \right]^+$ is the tightest constraint. The first inequality (b) follows since the rates achieved by the optimized powers must be larger than those achieved by one particular strategy that meets the constraints – in this case the strategy that yields the P_i^* which we construct in

Appendix .4. Inequality (c) follows from the fact that $2P_i^* \geq P_i$, as also shown in Appendix .4. Finally, we bound $\frac{1}{2} \log \left(\frac{3P_1^*}{N_2} \right)$ with $\frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right)$ as follows: If $\frac{P_1}{N_2} \geq 2$, it follows that $\frac{P_1^*}{N_2} \geq 1$, and hence $\frac{1}{2} \log \left(\frac{3P_1^*}{N_2} \right) \geq \frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right)$. Otherwise, $\frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right) < \frac{1}{2} \log 3$. Similarly, we may bound $\frac{1}{2} \log \left(\frac{3P_3^*}{N_4} \right)$ and $\frac{1}{2} \log \left(\frac{3P_3^*}{N_2} \right)$ with $\frac{1}{2} \log \left(1 + \frac{P_3}{N_4} \right)$ and $\frac{1}{2} \log \left(1 + \frac{P_3}{N_2} \right)$ respectively.

Remark 5 *We achieve a constant gap to capacity for the symmetric rate of $\frac{1}{2} \log(3)$ bit/s/Hz. The only other scheme we are aware of that has been shown to achieve a constant gap is noisy network coding (13) which achieves a larger gap of 1.26 bits/s/Hz to the capacity. The improvement in rates of the proposed scheme may be attributed to the removal of the noise at intermediate relays (it is a lattice based Decode and Forward scheme) without the sum-rate constraints that would be needed in i.i.d. random coding based Decode-and-Forward schemes.*

6.5 Extensions to half-duplex channels and more than two relays

We now extend our results to half-duplex channels and to two-way relay channels with more than two relays.

6.5.1 Half-duplex

The proposed lattice coding scheme may be generalized to channels with half-duplex nodes, i.e. in which a node may either transmit or receive at a given time but not both. The scheme is illustrated in Figure 17, where we see that the proof generally mimics the full-duplex case (Theorem 19, Lemma 20 and Theorem 21), but that each phase (or block) in the full-duplex

case is divided into two phases / blocks in the half-duplex case, as nodes may not transmit and receive at the same time. Thus, one may achieve half the rates as in the full duplex case, i.e.

$$R_a, R_b < R_{half-duplex} = \frac{1}{2} R_{achievable},$$

where $R_{achievable}$ is expressed in Theorem 21.

6.5.2 More than two relays

This lattice coding scheme may also be generalized to more than two relays. For example, for the Two-way Three-relay Channel with five nodes: $1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4 \leftrightarrow 5$, we may apply the same strategy by aligning the codewords between 1 and 3, 3 and 5, and 2 and 4 (i.e. nest the corresponding codebooks). To align or nest the codebooks, one may truncate the transmit powers so that $\frac{P'_1}{P'_3}$, $\frac{P'_3}{P'_5}$ and $\frac{P'_2}{P'_4}$ are either squares, or the reciprocals of squares of integers. By extending our Block Markov strategy, the final achievable rate region would be:

$$R_a, R_b < \max_{\substack{P'_i \leq P_i, \\ \frac{P'_1}{P'_3} = N^2 \text{ or } \frac{1}{N^2}, \\ \frac{P'_2}{P'_4} = M^2 \text{ or } \frac{1}{M^2}, \\ \frac{P'_3}{P'_5} = K^2 \text{ or } \frac{1}{K^2}}} \min_{k = \{1, 2, 3, 4\}, j = \{2, 3, 4, 5\}} \left(\left[\frac{1}{2} \log \left(\frac{P'_k}{N_{k+1}} \right) \right]^+, \left[\frac{1}{2} \log \left(\frac{P'_j}{N_{j-1}} \right) \right]^+ \right).$$

where $M, N, K \in \mathbb{Z}^+$ and $i = \{1, 2, 3, 4, 5\}$.

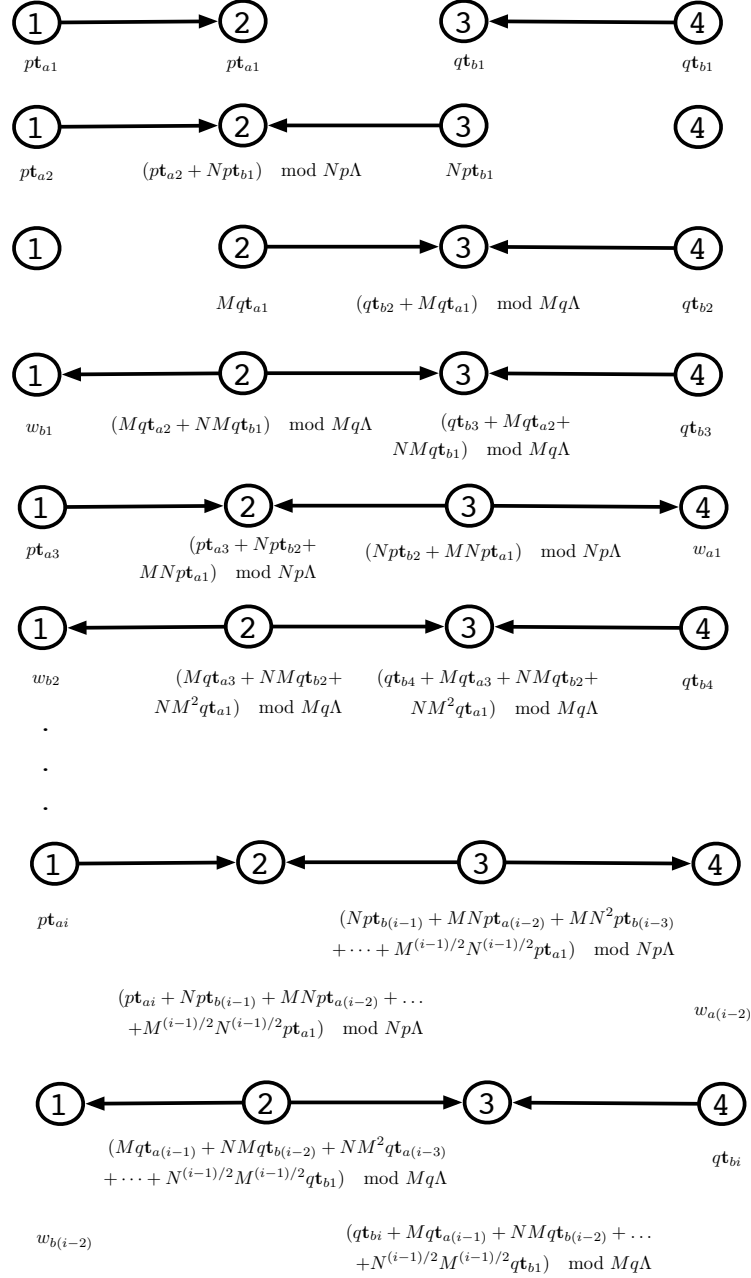


Figure 17. Half-duplex case.

CHAPTER 7

CONCLUSION

We have demonstrated that lattice codes may mimic random Gaussian codes in the context of the Gaussian relay channel, achieving the same Decode-and-Forward and Compress-and-Forward rates as those using random Gaussian codes. One of the central technical tools needed for Decode-and-Forward was a new lattice list decoder, which proved useful in networks with cooperation where various links to a destination carry different encodings of a given message. The DF scheme is further extended to multiple relay scenario. In Compress-and-Forward scheme, we incorporate lattice Wyner-Ziv scheme to achieve the CF rate.

For the scenarios with multiple sources, we have further demonstrated a technique for combining the linearity of lattice codes with classical Block Markov cooperation techniques in a DF fashion in the multiple-access relay channel and the two-way relay channel with direct links. These achievability schemes outperform known i.i.d. random coding based schemes for certain channel conditions. Moreover, we proposed a lattice coding scheme for the AWGN Two-way Two-relay Channel ($1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4$) which achieves within $\frac{1}{2} \log 3$ bit/Hz/s from the symmetric rate capacity. This scheme may be generalized to half-duplex nodes, and two-way channels with more than two relays. In our scheme, each relay decodes a sum of codewords as all transmitted signals are properly chosen lattice codewords, performs the “Re-distribution Transform” which maps the decoded lattice point to another so as to fully utilize its transmit power, and

broadcasts this transformed, scaled, lattice codeword. All decoders are lattice decoders and only a single nested lattice codebook pair is needed in our scheme.

In summary, lattice codes have been considered and proved to be a promising coding scheme for the wireless Gaussian networks, especially for the complex network structure involving relay nodes. The thesis shows that lattice codes can perform as well as, and even outperform currently known achievability based schemes based on i.i.d. random codes in many Gaussian relay networks from a theoretical point of view. An interesting open problem is how to exploit some of these beneficial properties of lattice codes in real communications systems. Practical lattice codes are being developed in (66; 67) and related physical-layer network coding ideas are presented in (68; 69) for relay networks, which provide a good start to this interesting question.

APPENDICES

.1 Details in Decoding step 2. of Theorem 7.

In applying the Lattice List Decoder of Theorem 3 to the steps between (Equation 4.23) – (Equation 4.26), we form the list

$$L_{R-D}^{w_{b-1}}(\mathbf{Y}_D(b)) = \{w_{b-1} \mid \mathbf{t}_2(w_{b-1}) \in S_{\kappa\mathcal{V}_{s2}, \kappa\Lambda_{c2}}(\mathbf{Y}'_D(b)) \mod \kappa\Lambda_2\},$$

where

$$\begin{aligned} \mathbf{Y}'_D(b) &= (\beta\mathbf{Y}_D(b) + \kappa\mathbf{U}_2(b-1)) \mod \kappa\Lambda_2 \\ &= (\kappa\mathbf{t}_2(w_{b-1}) - (1-\beta)\kappa\mathbf{X}'_2(w_{b-1}) + \beta(\mathbf{X}'_1(w_b) + \mathbf{Z}_D(b))) \mod \kappa\Lambda_2. \end{aligned}$$

As in Section 6.1.1, choose β to be the MMSE coefficient $\beta_{MMSE} = \frac{\kappa^2\bar{\alpha}P}{\kappa^2\bar{\alpha}P + \alpha P + N_D}$, resulting in self-noise $\mathbf{Z}_{eq} := ((1-\beta)\kappa\mathbf{X}'_2(w_{b-1}) + \beta(\mathbf{X}'_1(w_b) + \mathbf{Z}_D(b))) \mod \kappa\Lambda_2$ of variance

$$N_{eq} = \frac{\kappa^2\bar{\alpha}P(\alpha P + N_D)}{\kappa^2\bar{\alpha}P + \alpha P + N_D}.$$

Select Λ_{s2} in the lattice chain $\Lambda_2 \subseteq \Lambda_{s2} \subseteq \Lambda_{c2}$ to have a fundamental Voronoi region of volume $V_{s2} = \left(\frac{\alpha P + N_D}{\alpha P + N_D + (\sqrt{\bar{\alpha}P} + \sqrt{P_R})^2}\right)^{n/2} V_2$ asymptotically (notice $V_{s2} < V_2$ as needed). This will ensure a list of the desired size $2^{n(R-R_R)}$ as long as $R_R < C((\sqrt{\bar{\alpha}P} + \sqrt{P_R})^2/(\alpha P + N_D))$. For rates R approaching $\frac{1}{2} \log \left(1 + \frac{P+P_R+2\sqrt{\bar{\alpha}PP_R}}{N_D}\right)$ (where list decoding is needed / relevant), $V_{c2} = \left(\frac{N_D}{P+P_R+2\sqrt{\bar{\alpha}PP_R+N_D}}\right)^{n/2} V_2$ asymptotically. Thus $V_{c2} < V_{s2} < V_2$ as needed.

Encoding:	block 1	block 2	block 3	block 4	block 5	block 6
①	$X'_1(w_1) + X'_2(1) + X'_3(1)$	$X'_1(w_2) + X'_2(w_1) + X'_3(1)$	$X'_1(w_3) + X'_2(w_2) + X'_3(w_1)$	$X'_1(w_4) + X'_2(w_3) + X'_3(w_2)$	$X'_1(1) + X'_2(w_4) + X'_3(w_3)$	$X'_1(1) + X'_2(1) + X'_3(w_4)$
②	$X'_2(1) + X'_3(1)$	$X'_2(w_1) + X'_3(1)$	$X'_2(w_2) + X'_3(w_1)$	$X'_2(w_3) + X'_3(w_2)$	$X'_2(w_4) + X'_3(w_3)$	$X'_2(1) + X'_3(w_4)$
③	$X'_3(1)$	$X'_3(1)$	$X'_3(w_1)$	$X'_3(w_2)$	$X'_3(w_3)$	$X'_3(w_4)$

Decoding:	block 1	block 2	block 3	block 4	block 5	block 6
②	w_1	w_2	w_3	w_4		
③	$L_{1-3}^{w_1}$	$L_{2-3}^{w_1}$ $L_{1-3}^{w_2}$	$L_{2-3}^{w_2}$ $L_{1-3}^{w_3}$	$L_{2-3}^{w_3}$ $L_{1-3}^{w_4}$	$L_{2-3}^{w_4}$	
④	$L_{1-4}^{w_1}$	$L_{2-4}^{w_1}$ $L_{1-4}^{w_2}$	$L_{3-4}^{w_1}$ $L_{2-4}^{w_2}$ $L_{1-4}^{w_3}$	$L_{3-4}^{w_2}$ $L_{2-4}^{w_3}$ $L_{1-4}^{w_4}$	$L_{3-4}^{w_3}$ $L_{2-4}^{w_4}$	$L_{3-4}^{w_4}$

Figure 18. Lattice Decode-and-Forward scheme for the AWGN multi-relay channel.

.2 Proof of Theorem 8

Proof: Here we demonstrate achievability for the permutation $\pi(2) = 2, \pi(3) = 3$, and thus drop $\pi(\cdot)$ to simplify notation. The other permutation may be analogously achieved. Source Node 1 transmits a message to the destination Node 4 with the help of two relays: Node 2 and Node 3. The achievability scheme follows a generalization of the lattice regular encoding/sliding window decoding DF scheme of Theorem 7. The only difference is the addition of one relay and thus one coding level.

Codebook construction: We construct three nested lattice chains according to Theorem 2:

- $\Lambda_1 \subseteq \Lambda_{s(1-3)} \subseteq \Lambda_{s(1-4)} \subseteq \Lambda_{c1}$, or $\Lambda_1 \subseteq \Lambda_{s(1-4)} \subseteq \Lambda_{s(1-3)} \subseteq \Lambda_{c1}$ (relative nesting order depends on the system parameters and will be discussed in the following paragraph)
- $\Lambda_2 \subseteq \Lambda_{s(2-3)} \subseteq \Lambda_{s(2-4)} \subseteq \Lambda_{c2}$, or $\Lambda_2 \subseteq \Lambda_{s(2-4)} \subseteq \Lambda_{s(2-3)} \subseteq \Lambda_{c2}$
- $\Lambda_3 \subseteq \Lambda_{s(3-4)} \subseteq \Lambda_{c3}$

How these are ordered depends on the relative values of the power split parameters $\alpha_1, \beta_1, \alpha_2 \in [0, 1]$, the power constraints P_1, P_2, P_3 and the noise variances N_2, N_3, N_4 . In particular, the second moments of coarse lattices are selected as: $\sigma^2(\Lambda_1) = \alpha_1 P_1$, $\sigma^2(\Lambda_2) = \beta_1 P_1$, and $\sigma^2(\Lambda_3) = (1 - \alpha_1 - \beta_1) P_1$. The message set $w \in \{1, 2, \dots, 2^{nR}\}$ is mapped in a one-to-one fashion to three codebooks $\mathbf{t}_1(w) \in \mathcal{C}_1 = \{\Lambda_{c1} \cap \mathcal{V}_1\}$, $\mathbf{t}_2(w) \in \mathcal{C}_2 = \{\Lambda_{c2} \cap \mathcal{V}_2\}$, and $\mathbf{t}_3(w) \in \mathcal{C}_3 = \{\Lambda_{c3} \cap \mathcal{V}_3\}$. These mappings are independent. The fine lattices $\Lambda_{c1}, \Lambda_{c2}, \Lambda_{c3}$ may be chosen to satisfy the needed rate constraint R by proper selection of the corresponding γ in Theorem 2. The lattices $\Lambda_{s(1-3)}, \Lambda_{s(2-3)}$ will be used for lattice list decoding at relay 3, while $\Lambda_{s(1-4)}, \Lambda_{s(2-4)}$, and $\Lambda_{s(3-4)}$ will be used for lattice list decoding at the destination node 4. They will all be Rogers good, with fundamental Voronoi region volume specified by the desired lattice list decoding constraints; we are able to select this volume (or equivalently second moment) arbitrarily as long as they are smaller than their corresponding nested coarse lattices, by Theorem 2. In which order they are nested will depend on the relative volumes, which in turn depends on the systems parameters $\alpha_1, \beta_1, \alpha_2 \in [0, 1]$, the power constraints P_1, P_2, P_3 and the noise variances N_2, N_3, N_4 .

Define the following signals (which will be superposed as described in the Encoding):

$$\mathbf{X}'_1(w_b) = (\mathbf{t}_1(w_b) + \mathbf{U}_1(b)) \mod \Lambda_1$$

$$\mathbf{X}'_2(w_b) = (\mathbf{t}_2(w_b) + \mathbf{U}_2(b)) \mod \Lambda_2$$

$$\mathbf{X}'_3(w_b) = (\mathbf{t}_3(w_b) + \mathbf{U}_3(b)) \mod \Lambda_3,$$

where \mathbf{U}_1 , \mathbf{U}_2 and \mathbf{U}_3 are the dithers which are uniformly distributed over \mathcal{V}_1 , \mathcal{V}_2 and \mathcal{V}_3 , respectively, independent from block to block, and independent of each other. The encoding and decoding steps are outlined in Figure 18. We make a small remark on our notation: \mathbf{X}'_i should not be thought of as the signal being transmitted by Node i (which would be \mathbf{X}_i but we do not use this, opting instead to write out the transmit signals in terms of \mathbf{X}'_i). Rather, Node i will send a superposition of the signals $\mathbf{X}'_i, \mathbf{X}'_{i+1}, \dots$. Thus, multiple nodes may transmit the same (scaled) codeword \mathbf{X}'_i which will coherently combine.

Encoding: We again use block Markov encoding: the message is divided into B blocks of nR bits each. In block b , suppose Node 2 knows $\{w_1, \dots, w_{b-1}\}$ and Node 3 knows $\{w_1, \dots, w_{b-2}\}$. Node 1 sends the superposition/sum of $\mathbf{X}'_1(w_b)$, $\mathbf{X}'_2(w_{b-1})$ and $\mathbf{X}'_3(w_{b-2})$ with power $\alpha_1 P_1$, $\beta_1 P_1$, and $(1 - \alpha_1 - \beta_1) P_1$ respectively. Node 2 sends the superposition/sum of $\sqrt{\frac{\alpha_2 P_2}{\beta_1 P_1}} \mathbf{X}'_2(w_{b-1})$ and $\sqrt{\frac{(1 - \alpha_2) P_2}{(1 - \alpha_1 - \beta_1) P_1}} \mathbf{X}'_3(w_{b-2})$ with power $\alpha_2 P_2$, and $(1 - \alpha_2) P_2$ respectively. Node 3 sends $\sqrt{\frac{P_3}{(1 - \alpha_1 - \beta_1) P_1}} \mathbf{X}'_3(w_{b-2})$ with power P_3 .

Decoding:

Node 2 decodes w_b : In block b , since Node 2 knows w_{b-1} and w_{b-2} and thus $\mathbf{X}'_2(w_{b-1})$ and $\mathbf{X}'_3(w_{b-2})$, it can subtract these terms from its received signal

$$\mathbf{Y}_2(b) = \mathbf{X}'_1(w_b) + \mathbf{X}'_2(w_{b-1}) + \mathbf{X}'_3(w_{b-2}) + \sqrt{\frac{P_3}{(1 - \alpha_1 - \beta_1)P_1}} \mathbf{X}'_3(w_{b-2}) + \mathbf{Z}_2(b)$$

and obtains a noisy observation of $\mathbf{X}'_1(w_b)$ only. Node 2 is able to then uniquely decode w_b as long as (see (25) or Lemma 6)

$$R < \frac{1}{2} \log \left(1 + \frac{\alpha_1 P_1}{N_2} \right).$$

Node 3 decodes w_{b-1} : Since Node 3 knows w_{b-2} and thus $\mathbf{X}'_3(w_{b-2})$, it subtracts these from $\mathbf{Y}_3(b)$:

$$\mathbf{Y}_3(b) = \mathbf{X}'_1(w_b) + \mathbf{X}'_2(w_{b-1}) + \mathbf{X}'_3(w_{b-2}) + \sqrt{\frac{\alpha_2 P_2}{\beta_1 P_1}} \mathbf{X}'_2(w_{b-1}) + \sqrt{\frac{(1 - \alpha_2) P_2}{(1 - \alpha_1 - \beta_1) P_1}} \mathbf{X}'_3(w_{b-2}) + \mathbf{Z}_3(b)$$

and obtains a noisy observation of $\mathbf{X}'_1(w_b)$ and $\mathbf{X}'_2(w_{b-1})$,

$$\mathbf{Y}_3^*(b) = \mathbf{X}'_1(w_b) + \left(1 + \sqrt{\frac{\alpha_2 P_2}{\beta_1 P_1}} \right) \mathbf{X}'_2(w_{b-1}) + \mathbf{Z}_3(b).$$

It then uses $\Lambda_{s(2-3)}$ to decode a list $L_{2-3}^{w_{b-1}}(\mathbf{Y}_3^*(b))$ of possible w_{b-1} of size $2^{n \left(R - C \left(\frac{(\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2})^2}{\alpha_1 P_1 + N_3} \right) \right)}$ in the presence of interference $\mathbf{X}'_1(w_b)$ (uniformly distributed over the fundamental Voronoi region of a Rogers good lattice code) and Gaussian noise $\mathbf{Z}_3(b)$ (hence we may apply Theorem 3). It then intersects this list $L_{2-3}^{w_{b-1}}(\mathbf{Y}_3^*(b))$ with the list $L_{1-3}^{w_{b-1}}(\mathbf{Y}_3^{**}(b-1))$ of asymptotic

size $2^{n\left(R-C\left(\frac{\alpha_1 P_1}{N_3}\right)\right)}$ obtained in block $b-1$ by subtracting off the known signals dependent on w_{b-2}, w_{b-3} to obtain $\mathbf{Y}_3^{**}(b-1) = \mathbf{X}'_1(w_{b-1}) + \mathbf{Z}_3(b-1)$. To ensure a unique w_{b-1} in the intersection, by independence of the lists (based on the independent mappings of the messages to the codebooks \mathcal{C}_1 and \mathcal{C}_2), we need

$$\begin{aligned} R &< C \left(\frac{(\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2})^2}{\alpha_1 P_1 + N_3} \right) + C \left(\frac{\alpha_1 P_1}{N_3} \right) \\ &= C \left(\frac{\alpha_1 P_1 + (\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2})^2}{N_3} \right). \end{aligned}$$

After Node 3 decodes w_{b-1} , it further subtracts $\mathbf{X}'_2(w_{b-1})$ from its received signal and obtains a noisy observation of $\mathbf{X}'_1(w_b)$. It again uses the lattice list decoder using $\Lambda_{s(1-3)}$ to output a list $L_{1-3}^{w_b}(\mathbf{Y}_3^{**}(b))$ of w_b of size $2^{n\left(R-C\left(\frac{\alpha_1 P_1}{N_3}\right)\right)}$ which is used in block $b+1$ to determine w_b .

Node 4 decodes w_{b-2} : Finally, Node 4 intersects three lists to determine w_{b-2} . These three lists are again independent by the independent mapping of the messages to the codebooks \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_3 , where each corresponds to one of the three links (between node 1-4, 2-4, and 3-4). The first list $L_{3-4}^{w_{b-2}}(\mathbf{Y}_4(b))$ of w_{b-2} messages is obtained by list decoding using $\Lambda_{s(3-4)}$ on its received signal

$$\begin{aligned} \mathbf{Y}_4(b) &= \mathbf{X}'_1(w_b) + \mathbf{X}'_2(w_{b-1}) + \mathbf{X}'_3(w_{b-2}) + \sqrt{\frac{\alpha_2 P_2}{\beta_1 P_1}} \mathbf{X}'_2(w_{b-1}) \\ &\quad + \sqrt{\frac{(1-\alpha_2)P_2}{(1-\alpha_1-\beta_1)P_1}} \mathbf{X}'_3(w_{b-2}) + \sqrt{\frac{P_3}{(1-\alpha_1-\beta_1)P_1}} \mathbf{X}'_3(w_{b-2}) + \mathbf{Z}_4(b) \end{aligned}$$

which is a combination of scaled signals $\mathbf{X}'_1(w_b)$ and $\mathbf{X}'_2(w_{b-1})$ which are uniform over the fundamental Voronoi regions of Rogers good lattices and additive Gaussian noise $\mathbf{Z}_4(b)$, and is of size

$$|L_{3-4}^{w_{b-2}}(\mathbf{Y}_4(b))| = 2^{n \left(R - C \left(\frac{(\sqrt{(1-\alpha_1-\beta_1)P_1} + \sqrt{(1-\alpha_2)P_2} + \sqrt{P_3})^2}{\alpha_1 P_1 + (\sqrt{\beta_1}P_1 + \sqrt{\alpha_2}P_2)^2 + N_4} \right) \right)}.$$

The second list $L_{2-4}^{w_{b-2}}(\mathbf{Y}_4^*(b-1))$ is obtained in block $b-1$ and is of size $2^{n \left(R - C \left(\frac{(\sqrt{\beta_1}P_1 + \sqrt{\alpha_2}P_2)^2}{\alpha_1 P_1 + N_4} \right) \right)}$, while the third list $L_{1-4}^{w_{b-2}}(\mathbf{Y}_4^{**}(b-2))$ is obtained in block $b-2$ and is of size $2^{n \left(R - C \left(\frac{\alpha_1 P_1}{N_4} \right) \right)}$.

The formation of these lists is described next (they are formed analogously in blocks $b-1$ and $b-2$).

After the successful decoding of w_{b-2} in block b , node 4 decodes two more lists which are used in the blocks $b+1$ and $b+2$ to determine w_{b-1} and w_b respectively. Node 4 first subtracts the $\mathbf{X}'_3(w_{b-2})$ terms from its received signal $\mathbf{Y}_4(b)$ to obtain $\mathbf{Y}_4^*(b)$ and decodes a list of possible w_{b-1} from the terms $\mathbf{X}'_2(w_{b-1})$ using $\Lambda_{s(2-4)}$ in the presence of interference terms $\mathbf{X}'_1(w_b)$ which are uniformly distributed over Rogers good lattices and Gaussian noise (hence Theorem 3 applies). This list is denoted as $L_{2-4}^{w_{b-1}}(\mathbf{Y}_4^*(b))$ and is used in the block $b+1$ to determine w_{b-1} .

After Node 4 decodes w_{b-1} in the block $b+1$, it further subtracts the $\mathbf{X}'_2(w_{b-1})$ terms from $\mathbf{Y}_4^*(b)$ to obtain $\mathbf{Y}_4^{**}(b) = \mathbf{X}'_1(w_b) + \mathbf{Z}_4(b)$. It then uses $\Lambda_{s(1-4)}$ to decode a list of w_b , denoted as $L_{1-4}^{w_b}(\mathbf{Y}_4^{**}(b))$, which is used in block $b+2$ to determine w_b .

In block b , to ensure a unique message w_{b-2} in the intersection of the three independent lists, we need

$$\begin{aligned} R &< C \left(\frac{\left(\sqrt{(1-\alpha_1-\beta_1 P_1)} + \sqrt{(1-\alpha_2)P_2} + \sqrt{P_3} \right)^2}{\alpha_1 P_1 + \left(\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2} \right)^2 + N_4} \right) + C \left(\frac{\left(\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2} \right)^2}{\alpha_1 P_1 + N_4} \right) + C \left(\frac{\alpha_1 P_1}{N_4} \right) \\ &= C \left(\frac{\alpha_1 P_1 + \left(\sqrt{\beta_1 P_1} + \sqrt{\alpha_2 P_2} \right)^2 + \left(\sqrt{(1-\alpha_1-\beta_1 P_1)} + \sqrt{(1-\alpha_2)P_2} + \sqrt{P_3} \right)^2}{N_4} \right). \end{aligned}$$

.3 Multi-phase Block Markov achievability strategy for Lemma 20

The achievable rate region for Lemma 20 is the same as that for Theorem 19; the achievability strategy is essentially the same, with slight variations on the re-scaling to meet the different power constraints. The details of who transmits and decodes what in each phase is outlined in Figure 19.

.4 A particular choice of P_i^* and proof that $2P_i^* \geq P_i$ ($i \in \{1, 3\}$) in Theorem 21

WLOG, we assume $P_3 \geq P_1$. Then, $m^2 \leq \frac{P_3}{P_1} \leq (m+1)^2$ for some integer $m \in \mathbb{Z}^+$. Consider the following strategy for choosing P_i^* such that $\frac{P_3^*}{P_1^*}$ is a non-zero integer squared or the inverse of an integer squared: If $m^2 \leq \frac{P_3}{P_1} \leq m(m+1)$, we choose $P_3^* = m^2 P_1$ and $P_1^* = P_1$. Then $\frac{P_3^*}{P_1^*} = \frac{m^2 P_1}{P_1} = m^2 \geq \frac{m^2 P_1}{m(m+1)P_1} \geq \frac{1}{2}$. Thus, $2P_3^* \geq P_3$ and $P_1^* = P_1$. Otherwise if $m(m+1) \leq \frac{P_3}{P_1} \leq (m+1)^2$, we choose $P_1^* = \frac{1}{(m+1)^2} P_3$ and $P_3^* = P_3$. Then $\frac{P_1^*}{P_3^*} = \frac{P_3}{(m+1)^2 P_1} \geq \frac{m(m+1)P_1}{(m+1)^2 P_1} \geq \frac{1}{2}$. Thus $2P_1^* \geq P_1$ and $P_3^* = P_3$. In general, this strategy ensures that $2P_i^* \geq P_i$.

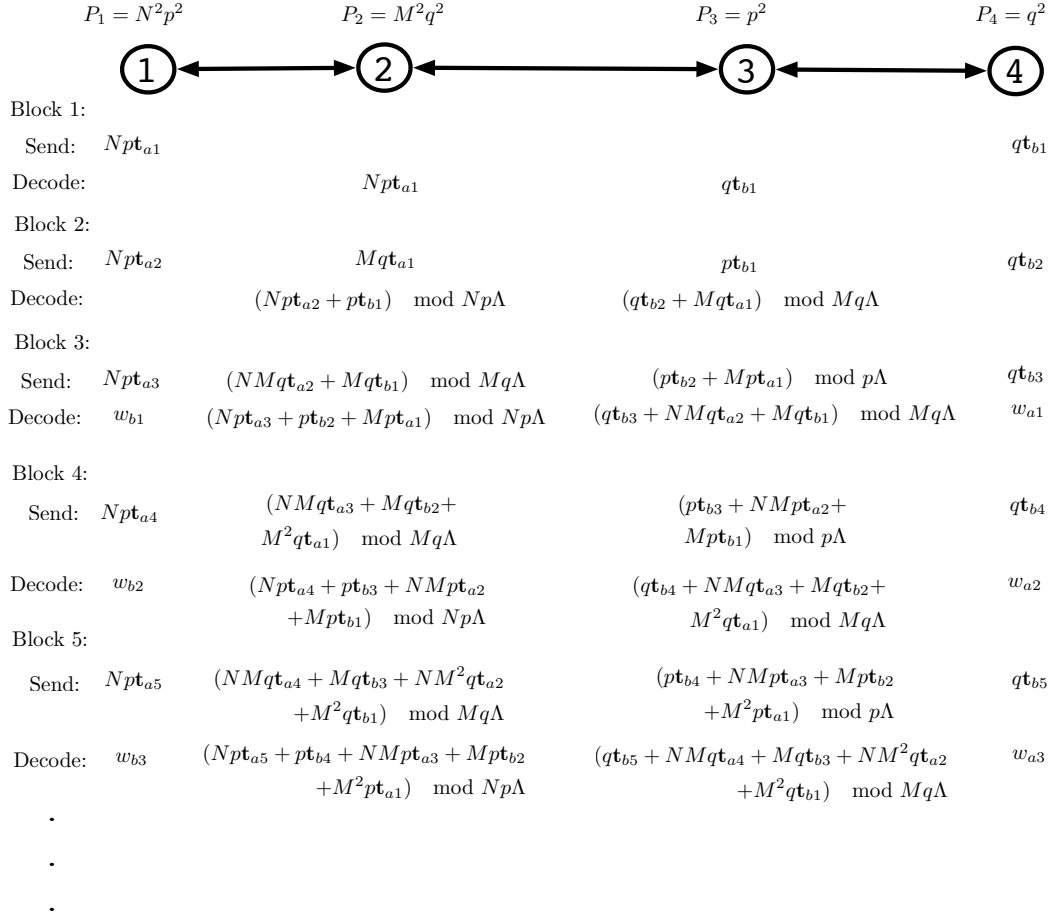


Figure 19. Multi-phase Block Markov achievability strategy for Lemma 20.

CITED LITERATURE

1. Nazer, B. and Gastpar, M.: Compute-and-forward: Harnessing interference through structured codes. IEEE Trans. Inf. Theory, 57(10):6463–6486, 2011.
2. Wilson, M. P., Narayanan, K., Pfister, H., and Sprintson, A.: Joint physical layer coding and network coding for bi-directional relaying. IEEE Trans. Inf. Theory, 56(11):5641–5654, November 2010.
3. Nam, W., Chung, S. Y., and Lee, Y.: Capacity of the Gaussian Two-Way Relay Channel to Within $1/2$ Bit. IEEE Trans. Inf. Theory, 56(11):5488–5494, November 2010.
4. Nam, W., Chung, S.-Y., and Lee, Y.: Nested lattice codes for gaussian relay networks with interference, 2009.
5. Özgür, A. and Diggavi, S.: Approximately achieving Gaussian relay network capacity with lattice codes. arXiv:1005.1284v1, 2010.
6. Nokleby, M. and Aazhang, B.: Lattice coding over the relay channel. In Proc. IEEE Int. Conf. Commun., Kyoto, Japan, June 2011.
7. Nokleby, M. and Aazhang, B.: Unchaining from the channel: Cooperative computation over multiple-access channels. In Proc. IEEE Inf. Theory Workshop, Paraty, Brazil, October 2011.
8. T. M. Cover and A. El Gamal: Capacity theorems for the relay channel. IEEE Trans. Inf. Theory, 25(5):572–584, September 1979.
9. L.-L. Xie and P. R. Kumar: A network information theory for wireless communication: scaling laws and optimal operation. IEEE Trans. Inf. Theory, 50(5):748–767, May 2004.
10. Kramer, G., Gastpar, M., and Gupta, P.: Cooperative strategies and capacity theorems for relay networks. IEEE Trans. Inf. Theory, 51(9):3037–3063, September 2005.
11. A. El Gamal and Y.-H. Kim: Lecture Notes on Network Information Theory. <http://arxiv.org/abs/1001.3404>, 2010.

CITED LITERATURE (Continued)

12. Xie, L.-L. and Kumar, P. R.: An achievable rate for the multiple-level relay channel. IEEE Trans. Inf. Theory, 51(4):1348–1358, 2005.
13. Lim, S.-H., Kim, Y.-H., El Gamal, A., and Chung, S.-Y.: Noisy network coding. IEEE Trans. Inf. Theory, 57(5):3132–3152, May 2011.
14. Bresler, G., Parekh, A., and Tse, D.: The approximate capacity of the many-to-one and one-to-many Gaussian interference channels. IEEE Trans. Inf. Theory, 56(9):4566–4592, 2010.
15. Sridharan, S., Jafarian, A., Vishwanath, S., and Jafar, S. A.: Capacity of symmetric k-user gaussian very strong interference channels.
16. Wyner, A. and Ziv, J.: The rate-distortion function for source coding with side information at the decoder. IEEE Trans. Inf. Theory, 22(1):1–10, 1976.
17. Zamir, R. and Shamai, S.: Nested linear/lattice codes for Wyner-Ziv encoding. In Proc. IEEE Inf. Theory Workshop, 1998.
18. Zamir, R., Shamai, S., and Erez, U.: Nested Linear/Lattice codes for structured multiterminal binning. IEEE Trans. Inf. Theory, 48(6):1250–1276, 2002.
19. Khormuji, M. and Skoglund, M.: On instantaneous relaying. IEEE Trans. Inf. Theory, 56(7):3378–3394, July 2010.
20. Yao, S., Khormuji, M., and Skoglund, M.: Sawtooth relaying. IEEE Commun. Lett., 12(9):612–615, September 2008.
21. Popovski, P. and Yomo, H.: Bi-directional amplification of throughput in a wireless multi-hop network. In Proc. IEEE Veh. Technol. Conf. - Spring, pages 588–593, Melbourne, May 2006.
22. Kim, S., Devroye, N., and Tarokh, V.: A class of bi-directional multi-relay protocols. In Proc. IEEE Int. Symp. Inf. Theory, pages 349–353, Seoul, June 2009.
23. Kim, S., Devroye, N., and Tarokh, V.: Bi-directional half-duplex protocols with multiple relays, 2008.
24. Pooniah, J. and Xie, L.-L.: An achievable rate region for the two-way two-relay channel. In Proc. IEEE Int. Symp. Inf. Theory, pages 489–493, July 2008.

CITED LITERATURE (Continued)

25. Erez, U. and Zamir, R.: Achieving $\frac{1}{2}\log(1 + SNR)$ on the AWGN channel with lattice encoding and decoding. IEEE Trans. Inf. Theory, 50(10):2293–2314, October 2004.
26. Erez, U., Litsyn, S., and Zamir, R.: Lattices which are good for (almost) everything. IEEE Trans. Inf. Theory, 51(10):3401–3416, 2005.
27. Zamir, R.: Lattices are everywhere. In 4th Annual Workshop on Information Theory and its Applications, UCSD, 2009.
28. Gel'fand, S. and Pinsker, M.: Coding for channels with random parameters. Probl. Contr. and Inf. Theory, 9(1):19–31, 1980.
29. Costa, M.: Writing on dirty paper. IEEE Trans. Inf. Theory, IT-29:439–441, May 1983.
30. Philosof, T., Zamir, R., and Khisti, A.: Lattice strategies for the dirty multiple access channel. Submitted to IEEE Trans. Inf. Theory, 2009.
31. Jafarian, A. and Vishwanath, S.: Gaussian interference networks: Lattice alignment. In Proc. IEEE Inf. Theory Workshop, pages 1–5, 2010.
32. Ordentlich, O., Erez, U., and Nazer, B.: The approximate sum capacity of the symmetric K-user gaussian interference channel, June 2012.
33. Krithivasan, D. and Pradhan, S.: Lattices for distributed source coding: Jointly gaussian sources and reconstruction of a linear function. IEEE Trans. Inf. Theory, 55(12):5628–5651, 2009.
34. Wagner, A.: On distributed compression of linear functions. IEEE Trans. Inf. Theory, 57(1):79–94, 2011.
35. Korner, J. and Marton, K.: How to encode the modulo-two sum of binary sources. IEEE Trans. Inf. Theory, 25(2):219–221, 1979.
36. Avestimehr, A., Diggavi, S., and Tse, D.: Wireless network information flow: a deterministic approach. IEEE Trans. Inf. Theory, 57(4):1872–1905, 2011.
37. Nazer, B., Gastpar, M., Jafar, S. A., and Vishwanath, S.: Ergodic interference alignment. IEEE Trans. Inf. Theory, 2012. to appear.

CITED LITERATURE (Continued)

38. Niesen, U., Nazer, B., and Whiting, P.: Computation Alignment: Capacity Approximation without Noise Accumulation.
39. Khormuji, M. and Skoglund, M.: Noisy analog network coding for the two-way relay channel. In Proc. IEEE Int. Symp. Inf. Theory, 2011.
40. Fong, S. L., Ping, L., and Sung, C. W.: Amplify-and-modulo for gaussian two-way relay channel. In Proc. 2nd International Workshop on Network Coding in Wireless Relay Networks (NRN), 2012.
41. Sankar, L., Kramer, G., and Mandayam, N.: Offset encoding for multiple-access relay channels. IEEE Trans. Inf. Theory, 53(10):3814–3821, October 2007.
42. Woldegebreal, D. and Karl, H.: Multiple-access relay channel with network coding and non-ideal source-relay channels. In Wireless Communication Systems, 2007. ISWCS 2007. 4th International Symposium on, pages 732–736, 2007.
43. Shannon, C.: A mathematical theory of communication. Bell Syst. Tech. J., 27(379-423, 623-656), Jul., Oct. 1948.
44. Cover, T. and Thomas, J.: Elements of Information Theory: Second Edition. Wiley, 2006.
45. Loeliger, H.: Averaging bounds for lattices and linear codes. IEEE Trans. Inf. Theory, 43(6):1767–1773, 1997.
46. Zamir, R. and Feder, M.: On lattice quantization noise. IEEE Trans. Inf. Theory, 42:1152–1159, 1996.
47. Poltyrev, G.: On coding without restrictions for the AWGN channel. IEEE Trans. Inf. Theory, 40(2):409–417, 1994.
48. Rogers, C. A.: Lattice coverings of space. Mathematica, 6:33–39, 1959.
49. Erez, U., Litsyn, S., and Zamir, R.: Lattices which are good for (almost) everything. IEEE Trans. Inf. Theory, 51(10):3401–3416, October 2005.
50. G. D. Forney Jr.: On the role of MMSE estimation in approaching the information theoretic limits of linear Gaussian channels: Shannon meets Wiener. In Proc. Allerton Conf. Commun., Control and Comp., 2003.

CITED LITERATURE (Continued)

51. Coppel, W.: Number Theory: An introduction to mathematics. Springer, 2 edition, 2009.
52. Carleial, A.: Multiple-access channels with different generalized feedback signals. IEEE Trans. Inf. Theory, 28(6):841–850, 1982.
53. Willems, F.: Information Theoretical Results for Multiple Access Channels. Doctoral dissertation, K.U. Leuven, 1982.
54. A. El Gamal and Y.-H. Kim: Network Information Theory. Cambridge University Press, 2011.
55. Kim, S., Devroye, N., Mitran, P., and Tarokh, V.: Achievable rate regions and performance comparison of half duplex bi-directional relaying protocols. IEEE Trans. Inf. Theory, 2011. to appear.
56. Avestimehr, A., Sezgin, A., and Tse, D.: Capacity of the two-way relay channel within a constant gap. European Transactions on Telecommunications, 21(4):363–374, 2010.
57. Baik, I. and Chung, S.-Y.: Network coding for two-way relay channels using lattices. In Proc. IEEE Int. Conf. Commun., Beijing, May 2008.
58. Ong, L., Kellett, C., and Johnson, S.: Capacity Theorems for the AWGN Multi-Way Relay Channel.
59. Xie, L.-L.: Network coding and random binning for multi-user channels. In Proc. of CWIT, pages 85–88, 2007.
60. Rankov, B. and Wittneben, A.: Achievable rate regions for the two-way relay channel. In Proc. IEEE Int. Symp. Inf. Theory, pages 1668–1672, Seattle, July 2006.
61. Nokleby, M., Nazer, B., Aazhang, B., and Devroye, N.: Relays that cooperate to compute. In International Symposium on Wireless Communication Systems, August 2012.
62. Song, Y. and Devroye, N.: List decoding for nested lattices and applications to relay channels. In Proc. Allerton Conf. Commun., Control and Comp., Monticello, IL, September 2010.
63. Ordentlich, O. and Erez, U.: Interference alignment at finite snr. Arxiv preprint arXiv:1104.5456, 2011.

CITED LITERATURE (Continued)

64. Wyner, A.: The rate-distortion function for source coding with side information at the decoder\ 3-II: General sources. Information and Control, 38(1):60–80, 1978.
65. Song, Y. and Devroye, N.: Lattice codes for the gaussian relay channel: Decode-and-forward and compress-and-forward. <http://arxiv.org/abs/1111.0084>, 2011.
66. Sommer, N., Feder, M., and Shalvi, O.: Low-density lattice codes. IEEE Trans. Inf. Theory, 54(4):1561–1585, April 2008.
67. Shalvi, O., Sommer, N., and Feder, M.: Signal codes: Convolutional lattice codes. IEEE Trans. Inf. Theory, 57(8):5203–5226, August 2011.
68. Koike-Akino, T., Popovski, P., and Tarokh, V.: Optimized constellations for two-way relaying with physical network coding. IEEE J. Select. Areas Commun., 27(5):773–787, June 2009.
69. Feng, C., Silva, D., and Kschischang, F. R.: Algebraic approach to physical-layer network coding. <http://arxiv.org/abs/1108.1695>, 2011.
70. Kim, S., Smida, B., and Devroye, N.: Capacity bounds on multi-pair two-way communication with a base-station aided by a relay. Submitted to IEEE Trans. Inf. Theory, July 2010.
71. U.Erez and Zamir, R.: Achieving $1/2\log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding . IEEE Trans. Inf. Theory, 2004.
72. Kim, Y. H., Sutivong, A., and Sigurjossón, S.: Multiple user writing on dirty paper. In Proc. IEEE Int. Symp. Inf. Theory, 2004.
73. Akhbari, B., Mirmohseni, M., and Aref, M. R.: Compress-and-Forward strategy for the relay channel with non-causal state information. In Proc. IEEE Int. Symp. Inf. Theory, 2009.
74. Zaidi, A., Shamai, S., Piantanida, P., and Vandendorpe, L.: Bounds on the capacity of the relay channel with noncausal state information at source. In Proc. IEEE Int. Symp. Inf. Theory, 2010.
75. Philosof, T., Zamir, R., Erez, U., and Khisti, A.: Lattice strategies for the dirty multiple access channel, 2009.

CITED LITERATURE (Continued)

- 76. Krithivasan, D. and Pradhan, S. S.: Lattices for distributed source coding: Jointly gaussian sources and reconstruction of a linear function, 2009.
- 77. Nazer, B. and Gastpar, M.: Reliable physical layer network coding. Proceedings of the IEEE, (99):1–23, 2011.
- 78. Song, Y. and Devroye, N.: A lattice Compress-and-Forward strategy for canceling known interference in Gaussian multi-hop channels. In Proc. Conf. on Inf. Sci. and Sys. (CISS), January 2011.
- 79. Song, Y. and Devroye, N.: Structured interference-mitigation in two-hop networks. In Proc. Workshop on Info. Theory and Applications, La Jolla, 2011.
- 80. Carleial, A. B.: Multiple-access channels with different generalized feedback signals. IEEE Trans. Inf. Theory, 28(6):841–850, November 1982.
- 81. Xie, L.-L.: Network coding and random binning for multi-user channels. In Proc. of the 10th Canadian Workshop on Inform. Theory, pages 85–89, June 2007.
- 82. Krithivasan, D. and Pradhan, S. S.: Distributed Source Coding Using Abelian Group Codes: A New Achievable Rate-Distortion Region. IEEE Trans. Inf. Theory, 57(3):1459–1591, March 2011.

VITA

Name	Yiwei Song
Education	University of Illinois at Chicago Ph.D. in Electrical Engineering (2009 - 2013) Nanjing University of Posts and Telecommunications Bachelor in Network Engineering (2005 -2009)
Experience	Broadcom Corporation System Design Intern (04/2013 - 08/2013) Samsung Information System America Research Intern (06/2012 - 08/2012)
Publications	Y. Song and N. Devroye, "Lattice Codes for Gaussian Relay Channels: Decode-and-Forward and Compress-and-Forward," accepted for publication on <i>IEEE Trans. Inform. Theory</i> , 2013. Y. Song, N. Devroye, H. Shao and C. Ngo, "Lattice Coding for the Two-way Two-Relay Channel," going to be submitted to <i>IEEE Trans. Wireless Comm.</i> , 2013. Y. Chen, Y. Song and N. Devroye, "The Capacity Region of Inverse-Compute-and-Forward Channels: Recovering Messages from Equations," going to be submitted to <i>IEEE Trans. Inform. Theory</i> , 2013.

VITA (Continued)

Y. Song, N. Devroye, H. Shao, C. Ngo, “Lattice Coding for the Two-way Two-Relay Channel,” *International Symposium on Information Theory*, Istanbul, July 2013.

Y. Chen, Y. Song and N. Devroye “The Capacity Region of Three User Gaussian Inverse-Compute-and-Forward Channels,” *International Symposium on Information Theory*, Istanbul, July 2013.

Y. Song and N. Devroye, “A Lattice Compress-and-Forward Scheme,” *Information Theory Workshop*, Paraty, Brazil October 2011.

Y. Song, N. Devroye, and B. Nazer, “Inverse Compute-and-Forward: Extracting Messages from Simultaneously Transmitted Equations,” *International Symposium on Information Theory*, St. Petersburg, August 2011.

Y. Song and N. Devroye, “A Lattice Compress-and-Forward Strategy for Canceling Known Interference in Gaussian Multi-hop Channels,” *45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, March 2011.

Y. Song and N. Devroye, “Structured Interference-Mitigation in Two-hop Networks,” *Information Theory and Applications Workshop*, UCSD, San Diego February 2011. (*invited*)

VITA (Continued)

Y. Song and N. Devroye, “List Decoding for Nested Lattices and Applications to Relay Channels,” *48th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, September 2010. *(invited)*

Presentations

“Further Comments on Lattice codes for Gaussian relay channels,” *invited to the BIRS workshop Algebraic Structure in Network Information Theory*, August 2011.

“Lattice Coding for Gaussian Relay Channels,” *Fourth Annual School of Information Theory*, May 2011.

“Lattice Coding for Compress-and-Forward,” *45th Annual Conference on Information Sciences and Systems (CISS)*, March 2011.

“List Decoding for Nested Lattices and Applications to Relay Channels,” *Third Annual School of Information Theory*, August 2010.