CROSS LAYER CODING SCHEMES FOR BROADCASTING AND RELAYING

A Dissertation

by

MAKESH PRAVIN JOHN WILSON

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2010

Major Subject: Electrical Engineering

CROSS LAYER CODING SCHEMES FOR BROADCASTING AND RELAYING

A Dissertation

by

MAKESH PRAVIN JOHN WILSON

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Krishna R. Narayanan
Committee Members,	Tie Liu
	Alexander Sprintson
	Natarajan Sivakumar
Head of Department,	Costas N. Georghiades

May 2010

Major Subject: Electrical Engineering

ABSTRACT

Cross Layer Coding Schemes for Broadcasting and Relaying. (May 2010)
Makesh Pravin John Wilson, B.E., College of Engineering Guindy, Anna University
Chair of Advisory Committee: Dr. Krishna R. Narayanan

This dissertation is divided into two main topics. In the first topic, we study the joint source-channel coding problem of transmitting an analog source over a Gaussian channel in two cases - (i) the presence of interference known only to the transmitter and (ii) in the presence of side information about the source known only to the receiver. We introduce hybrid digital analog forms of the Costa and Wyner-Ziv coding schemes. We present random coding based schemes in contrast to lattice based schemes proposed by Kochman and Zamir. We also discuss superimposed digital and analog schemes for the above problems which show that there are infinitely many schemes for achieving the optimal distortion for these problems. This provides an extension of the schemes proposed by Bross and others to the interference/source side information case. The result of this study shows that the proposed hybrid digital analog schemes are more robust to a mismatch in channel signal-to-noise ratio (SNR), than pure separate source coding followed by channel coding solutions. We then discuss applications of the hybrid digital analog schemes for transmitting under a channel SNR mismatch and for broadcasting a Gaussian source with bandwidth compression. We also study applications of joint source-channel coding schemes for a cognitive setup and also for the setup of transmitting an analog Gaussian source over a Gaussian channel, in the presence of an eavesdropper.

In the next topic, we consider joint physical layer coding and network coding solutions for bi-directional relaying. We consider a communication system where two transmitters wish to exchange information through a central relay. The transmitter and relay nodes exchange data over synchronized, average power constrained additive white Gaussian noise channels. We propose structured coding schemes using lattices for this problem. We study two decoding approaches, namely lattice decoding and minimum angle decoding. Both the decoding schemes can be shown to achieve the upper bound at high SNRs. The proposed scheme can be thought of as a joint physical layer, network layer code which outperforms other recently proposed analog network coding schemes. We also study extensions of the bi-directional relay for the case with asymmetric channel links and also for the multi-hop case. The result of this study shows that structured coding schemes using lattices perform close to the upper bound for the above communication system models.

To my father and mother

ACKNOWLEDGMENTS

I would like to express my sincere thanks to my committee chair, Dr. Krishna Narayanan, for his guidance throughout my research work. I am deeply indebted to him for his kindness, patience and encouragement. I am extremely thankful to him for mentoring me during the many challenging times in my research. I am also very thankful to him, for providing me with immense freedom in my choice of research topic, and also for the very generous financial support towards my graduate study at Texas A&M. I would also like to thank the members in my committee, Dr. Alex Sprintson, Dr. Tie Liu and Dr. Natarajan Sivakumar, for their time, comments and positive feedback towards my dissertation work.

I would also like to thank Dr. Giuseppe Caire, Dr. Alexander Sprintson and Dr. Henry Pfister for the many fruitful interactions and ideas towards my research work. My thanks to Dr. Scott Miller, Dr. Costas Georghiades, Dr. Jean-Francois Chamberland, Dr. Srinivas Shakkotai, Dr. Bill Johnson, Dr. Roger Smith, members of my dissertation committee and several other professors in Texas A&M for teaching me some very interesting courses. My special thanks to our department staff, Mrs. Paula Evans, and Mrs. Tammy Carda. Also my thanks to the department and National Science Foundation for supporting me throughout my graduate school. My sincere thanks to several students in our wireless communication group for the enthusiastic interactions. I would like to thank Abhiram, Kapil, Nitin, Jing Jiang, Hari, Janath, Mothi, Karthic, Ananth, Momin, Mohammad, Hung Ly, Jae Won, Richa, Fan, Salim, Parimal, Daehyun and Mustafa for the interesting conversations on research and for the wonderful friendships.

I would also like to thank my roommates Sahil, Suganth, Karthic and Nagendra for the friendships outside school. I would like to thank the College Station community for the amazing hospitality, throughout my stay here. Specifically, I would like to thank the A&M Church of Christ for providing a welcoming atmosphere to international students through the International House (IHouse). I am also very thankful for the several friendships made through the IHouse. I would also like to express my sincere thanks to the families in College Station, the Closners, the Orozcos, the Delsignores, the Buffingtons, the Schultes and the Wilson's for always welcoming me for the several American festivals and making me feel at home.

Last but not the least, I would like to express my deepest thanks and regards for my parents and my sister, Brinda, for their ever present love and encouragement. Without the constant love of my parents and the rigorous academic training that they ingrained in me through childhood, this work would have never been possible.

TABLE OF CONTENTS

CHAPTER Page

LIST OF FIGURES

FIGURE Page

CHAPTER I

INTRODUCTION

A typical communication system has several distinct layers/blocks with different functionalities [1]. For example, the physical layer in a communication system deals with the transmission and reception of physical waveforms through a communication medium [2], and the network layer deals with the routing/mixing of digital data. The physical layer can be further split into a source coding block and a channel coding block. The source coding block deals with the conversion of the analog signal into compressed digital data, as in a digital video camera. The channel coding block deals with the transmission of the digital data reliably over a noisy channel.

Separate protocols are usually designed for each of these layers/blocks. This form of decomposition to different blocks/layers has been shown to be optimal for some cases. For example, the separation theorem [2] states that separate source coding followed by channel coding is optimal for the point to point communication system. However, in several other situations cross layer coding are shown to be advantageous and there has been an increased interest in studying these schemes [3–5]. The main theme in this dissertation is to show that for certain scenarios as discussed below, cross layer coding designs provide significant performance gains over pure separation based designs.

This dissertation is divided into two main topics. The first topic deals with combining source coding and channel coding ideas, and we introduce many joint source channel coding (JSCC) schemes. We show that the joint source-channel coding schemes are more robust in non-ergodic channels, compared to separation based

---

The journal model is *IEEE Transactions on Automatic Control.*

schemes. In the second topic, we show that joint physical layer and network layer coding schemes offers significant throughput gains over separate physical layer coding, followed by network layer coding schemes. In the following sections we present the main topics in more detail and provide an overview of the main results.

A. Joint source channel coding(JSCC)

We first present a motivation for studying joint source-channel coding schemes. Consider the classical problem of transmitting N samples of a discrete-time independent identically distributed (i.i.d) zero mean real Gaussian source $\mathbf{v}$ in N uses of an additive white Gaussian noise (AWGN) channel such that the mean-squared error distortion is minimized. Let the source be encoded into the sequence $\mathbf{x}$ which satisfies a power constraint, namely $E[\mathbf{x}\mathbf{x}^T] \leq NP$. Let the output of the AWGN channel $\mathbf{y}$ be given by

$$\mathbf{y} = \mathbf{x} + \mathbf{w},$$

where $\mathbf{w}$ is a noise vector of i.i.d Gaussian random variables with zero mean and variance σ^2. If the source variance is σ_v^2, then the optimal mean-squared error distortion that can be achieved is $D_{opt} = \frac{\sigma_v^2}{1+\frac{P}{\sigma^2}}$. This optimal performance can be achieved by a simple scheme of separate source and channel coding [2].

In such a separation based scheme, the source is first quantized and the quantization index is transmitted using an optimal code for the AWGN channel. Though this scheme is optimal for the designed channel noise variance of σ^2, the scheme suffers from a marked *threshold effect* [6], when the actual channel noise variance σ_a^2 is different from the designed one. For example, if the actual channel signal-to-noise ratio(SNR) P/σ_a^2 is worse than the designed channel SNR of P/σ^2, i.e. $\sigma^2 < \sigma_a^2$, the channel code can not be decoded and we get a poor estimate of the analog source.

However, if the actual channel SNR is better than the designed channel SNR, i.e. $\sigma^2 > \sigma_a^2$, we still obtain the same distortion of $\frac{\sigma_v^2}{1+\frac{P}{\sigma^2}}$ in the estimate of the source. Though the channel has a better SNR, the distortion in the estimation of the source does not improve. This is due to the use of the fixed quantizer at the source. In other words, the separation scheme does not provide a graceful degradation of source distortion with the channel SNR.

A solution to this problem is to introduce an uncoded(analog) scheme [7, 8], where the source is not explicitly quantized. The source is scaled to match the transmit power constraint and transmitted over the channel without any coding. The receiver is assumed to have knowledge of the channel noise variance and forms a linear estimate of the source. This scheme can be shown to be optimal for the design channel and will also provide a graceful degradation of the source distortion with the channel SNR [7]. It can also be seen from the above example that the previous scheme considered is a joint source-channel coding scheme, and is shown to be more robust for non-ergodic channels, i.e., when the actual channel is different from the design channel.

Even though the above JSCC scheme is robust, it performs well only for the special source channel bandwidth matched case. This motivates us to study new JSCC schemes for a few different communication system models, other than the purely bandwidth matched case. One system model that we will consider is the communication of an analog source over a Gaussian channel in the presence of interference. The interference is assumed to be known at the transmitter, but is unknown at the receiver. We propose JSCC schemes for this system model. The schemes can be treated as an extension of Costa's dirty paper coding [9] for the joint source channel coding setup. Another model considered is the case where there is some side information about the source available at the receiver, but is unknown at the transmitter. We also consider cases when there is interference known only at the transmitter and source side-information known only at the receiver, and introduce JSCC schemes for the above setup.

We also study applications of the above schemes to broadcasting an analog source with bandwidth compression and broadcasting in a cognitive setup. We also propose JSCC schemes for secrecy systems that involve the transmission of an analog source in the presence of an eavesdropper. In the next section we present a brief overview of the bi-directional relaying problem.

B. Joint physical layer coding and network coding for bi-directional relaying

A bi-directional relay is composed of a wireless communication system, where two transmitters (say A and B) wish to exchange information with each other through a central half-duplex relay (say J) as shown in Fig. 1 below. The bi-directional relay can be treated as a building block of a general wireless network, as it captures succinctly its two chief features, namely its superposition nature and its broadcast nature. When the two nodes A and B transmit their respective signals simultaneously, the relay receives a superposition sum of the two signals. This essentially captures the superposition part and when the relay J transmits a signal and the other nodes listen, this captures the broadcast part.

We are interested in the problem of maximizing the rate of information exchange over the bi-directional relay. There are a few possible solutions to this problem. One naive solution is the transmission of the signals in four separate time slots. When each node transmits, the other nodes are silent. Hence the transmission takes place consecutively starting from node A to relay J, from node J to relay B, from node B to relay J and finally from relay J to node A in four separate time slots. The above setup involves purely physical layer coding with the relay just forwarding the packets.

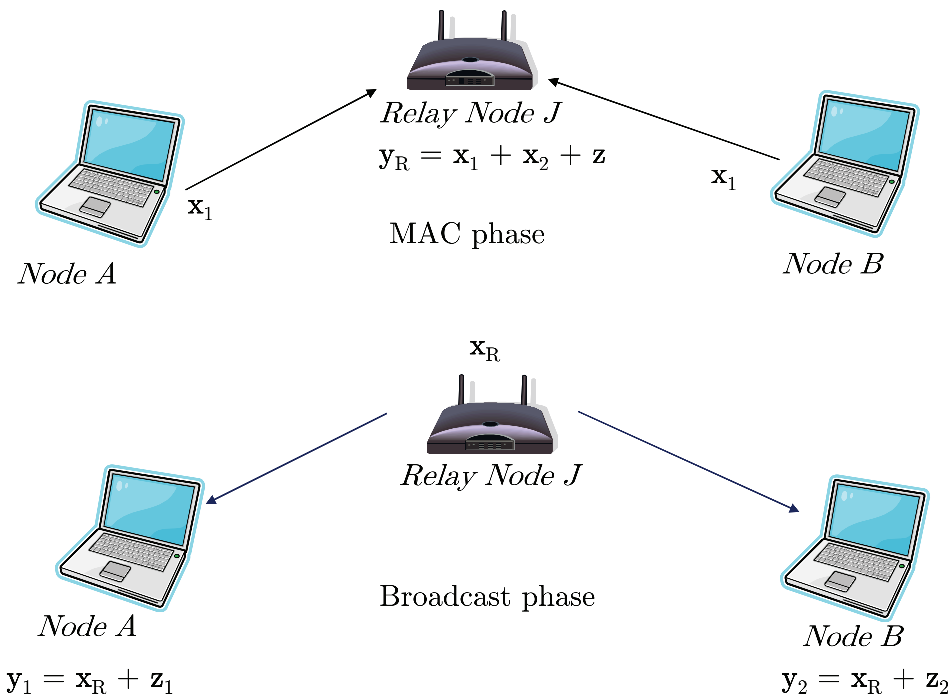

Fig. 1. Bi-directional relaying.

There is also a network coding solution [4] for the same problem. The transmission takes place in three time slots. In the first slot node A transmits while the other nodes are silent and in the second slot node B transmits, while the other nodes remain silent. The relay decodes the packets from node A and node B in the first two slots. During the third slot the relay performs an XOR of the packets and broadcasts it back to the nodes. The nodes can obtain their corresponding packets by a reverse XOR operation. This scheme therefore involves a separate physical layer coding and network coding.

In this dissertation we show that it is possible to obtain much higher data rates by performing the physical layer coding and network coding in a joint fashion. In our proposed scheme, both the nodes transmit simultaneously to the relay. The physical medium naturally mixes the signals. The relay instead of decoding to the individual packets decodes to a function of the transmitted signals. The relay then broadcasts the function of the transmitted signals in the next time slot. Each of the nodes can decode their individual messages from the received signal in the broadcast phase and also recover its own packet. If the function is chosen appropriately, the joint network coding and physical layer coding solution will perform very close to the upper bound for this problem.

To illustrate our proposed joint coding solution for bidirectional relaying, we first focus on the bidirectional relay with symmetric channel gains. We show that structured coding schemes based on nested lattices and nested lattice decoding achieves rates very close to the upper bound. We also analyze a different decoder namely a minimum angle decoder that also achieves rates close to the upper bound. We next consider the case of asymmetric channel gains and discuss schemes that perform close to the upper bound. Extensions to multiple hops are also discussed.

C. Overview of results

The main results in this dissertation are as follows.

JSCC results:

- We have proposed several joint source channel coding(JSCC) schemes for transmitting a Gaussian source over an AWGN channel under different side information scenarios, namely interference known only at the transmitter, side information about the source available only at the receiver and also the case where both interference known only at transmitter and side information of the source available only at the receiver. The schemes proposed can be treated as an extension of Costa's dirty paper coding and Wyner-Ziv coding for the JSCC setup.

- Both the JSCC schemes proposed in this dissertation and separation based schemes are optimal for a given design channel signal-to-noise ratio(SNR). However the JSCC schemes perform better when compared to the separation based schemes when the actual SNR of the channel turns out to be higher than the design SNR.

- We present application of the JSCC schemes discussed above for the problem of broadcasting an analog source with bandwidth compression.

- We propose JSCC schemes for communication with a physical layer secrecy requirement. We also study a cognitive setting, which consists of a secondary communication system that co-exists with a primary system. The secondary system is assumed to have some knowledge of the primary system and uses this knowledge to communicate efficiently without degrading the performance of the primary system. We propose JSCC schemes for the secondary system in the above setup.

Bi-directional relaying results:

- A nested lattice scheme is proposed for the symmetric bi-directional relaying problem and under nested lattice decoding it is shown that a rate of $\frac{1}{2}\log(\frac{1}{2}+\frac{P}{\sigma^2})$ can be exchanged between the nodes, where $\frac{P}{\sigma^2}$ is the channel SNR. This rate is shown to be very close to the upper bound of $\frac{1}{2}\log(1+\frac{P}{\sigma^2})$ at high signal to noise ratios.

- The nested lattice decoder performs decoding after an initial modulo operation. This may not necessarily be optimal, and hence a different decoder namely the minimum angle decoder that does not involve the modulo operation and is also analytically tractable is analyzed. It is shown that the minimum angle decoder achieves a rate of $\frac{1}{2}\log(\frac{1}{2}+\frac{P}{\sigma^2})$. Though the minimum angle decoder does not improve on the lattice decoder, its analysis provides a good geometric picture and shows that the sum of lattice points in high dimensions are concentrated in a thin spherical shell. This may prove insightful in understanding the lattice decoder at low signal to noise ratios.

- The bi-directional relay with asymmetric channel gains, whose fading coefficients are assumed to be known at the transmitter is considered. For this setup, an upper bound on the exchange rate is obtained. We next derive power allocation policies at the transmitter, and show that lattice based schemes coupled with our power allocation policy achieve the upper bound at high SNRs.

- A multi-hop scenario is considered which shows that the lattice based approach can be extended to exchanging information over multi-hops, and can achieve exchange rates close to the upper bound.

D. Organization of dissertation

The dissertation is split into two main topics, namely JSCC schemes for side information problems and joint physical layer coding and network coding for bi-directional relaying. JSCC schemes and some of it's applications are presented in chapters II and III. Chapter II introduces our proposed JSCC schemes and chapter III discusses some applications of our proposed schemes. Joint physical layer and network coding as applied to bi-directional relaying is discussed in chapters IV and V. In chapter IV, structured codes using lattices are proposed for the bi-directional relaying problem with symmetric channel gains. In chapter V, the bi-directional relaying problem is considered, where the channel gains are assumed to have asymmetric fading coefficients. Power allocation policies and lattice based coding schemes are proposed for this setup. Also we consider extensions of the bi-directional relaying to the multi-hop case in this chapter. Finally in chapter VI, we conclude the dissertation and point to future areas of work.

Throughout this dissertation, vectors are denoted by bold face letters such as $\mathbf{x}$. Upper case letters are used to denote scalar random variables. When considering a sequence of i.i.d random variables, a single upper case letter is used to denote each component of the random vector. For example, if X is a scalar random variable, then $\mathbf{x}$ is a vector containing independent realizations of X.

CHAPTER II

JSCC FOR SOME SIDE INFORMATION PROBLEMS

In this chapter, we study the problem of transmitting N samples of a real analog source $\mathbf{v} \in \mathbb{R}^N$, whose components are independent realizations of a random variable $V \sim \mathcal{N}(0, \sigma_v^2)$ in N uses of an AWGN channel with noise variance σ^2 in the presence of side information. It is assumed that there is an interference $\mathbf{s} \in \mathbb{R}^N$ which is known to the transmitter but unknown to the receiver. $\mathbf{s}$ is assumed to be the realization of a sequence of real i.i.d Gaussian random variables with zero mean and variance Q. It is also assumed that the receiver has knowledge of $\mathbf{v}' \in \mathbb{R}^N$, a side information of the source $\mathbf{v}$. $\mathbf{v}'$ is available only to the receiver and is assumed to be unknown to the transmitter. The correlation model between the side information $\mathbf{v}$ and $\mathbf{v}'$ is given by

$$\mathbf{v} = \mathbf{v}' + \mathbf{z}, \tag{2.1}$$

where $\mathbf{z} \in \mathbb{R}^N$ and $\mathbf{v}'$ are assumed to be i.i.d realization of two zero mean Gaussian random variables Z and V', respectively. Z and V' are assumed to be independent of each other and have a variance of σ_z^2 and $(\sigma_v^2 - \sigma_z^2)$, respectively. The input power to the channel $\mathbb{E}[X^2]$ is assumed to be constrained to be P. The received signal $\mathbf{y}$ is given by

$$\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w}, \tag{2.2}$$

where $\mathbf{s}$ is the interference and $\mathbf{w}$ is the AWGN. The metric of interest is the end to end average mean square distortion in the estimation of the source $\mathbf{v}$. We are interested in proposing joint source channel coding schemes which not only provide the optimal distortion for this setup, but also provide a better distortion performance when the actual noise variance of the channel is lesser than σ^2.

In [10], Kochman and Zamir have presented a lattice based hybrid digital analog(HDA) scheme for the above setup. The scheme proposed in our work is closely related to Kochman and Zamir's scheme, although our proposed scheme was developed independently and our scheme uses random coding instead of lattice codes considered in [10], and we derive our results from mutual information functionals. This provides a nice extension of Costa's dirty paper coding and Wyner-Ziv coding to the joint source channel coding setup and makes the relationship between the auxiliary random variable and the source more explicit. For an intuitive explanation of the binning schemes employed in dirty paper coding and Wyner-Ziv coding, the interested reader can refer appendix G.1.

We next present the main results in this chapter.

A. Main results

- We have proposed several joint source channel coding(JSCC) schemes for transmitting a Gaussian source over an AWGN channel under different side information scenarios. The case of channel interference known only at the transmitter is discussed in section B. The case of side information of the source available only at the receiver is presented in section C and also the case where both interference known only at transmitter and side information of the source available only at the receiver is discussed in section D. The schemes proposed can be treated as the extension of Costa's dirty paper coding and Wyner-Ziv coding for the JSCC setup.

- We show that there is a family of infinitely many schemes that are optimal for this problem which contain pure separation based schemes and JSCC schemes as special cases. This can be viewed as the extension of Bross, Lapidoth and Tinguely's [11] result in the presence of interference/side-information.

- The JSCC schemes proposed in this dissertation are optimal for a given design channel signal-to-noise ratio(SNR). However, the JSCC schemes perform better when compared to the separation based schemes when the actual SNR of the channel turns out to be higher than the design SNR. The performance of JSCC schemes under SNR variations is presented in section E.
- JSCC schemes for general sources and channels are also discussed in appendix 2.

B. JSCC with interference known at the transmitter

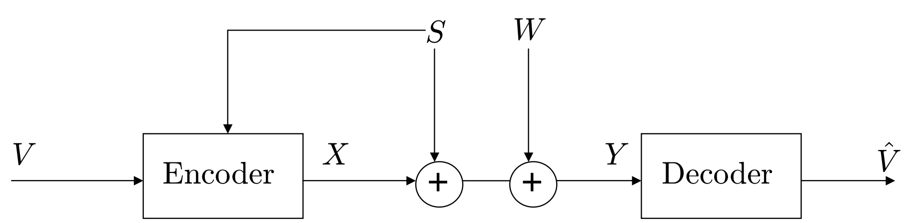

Fig. 2. Block diagram of the joint source channel coding problem with interference known only at the transmitter.

We first consider the problem of transmitting N samples of a real analog source $\mathbf{v} \in \mathbb{R}^N$, whose components are independent realizations of a random variable $V \sim \mathcal{N}(0, \sigma_v^2)$ in N uses of an AWGN channel with noise variance σ^2 in the presence of an interference $\mathbf{s} \in \mathbb{R}^N$ which is known to the transmitter but unknown to the receiver. Further, let us assume that $\mathbf{s}$ be the realization of a sequence of real i.i.d Gaussian random variables with zero mean and variance Q and let the input power to the channel $\mathbb{E}[X^2]$ be constrained to be P. The problem setup is shown schematically in

Fig. 2. The received signal $\mathbf{y}$ is given by

$$\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w} \tag{2.3}$$

where $\mathbf{s}$ is the interference and $\mathbf{w}$ is the AWGN.

The optimal distortion of $\frac{\sigma_v^2}{\left(1+\frac{P}{\sigma^2}\right)}$ can be obtained even in the presence of the interference by using the following (obvious) separate source and channel coding scheme.

1. Separation based scheme with Costa coding (digital Costa coding)

We first quantize the source using an optimal quantizer to produce an index $m \in \{1, 2, \ldots, 2^{NR}\}$, where $R = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right) - \epsilon$. Then, the index is transmitted using Costa's writing on dirty paper coding scheme [9]. Since the quantizer output is digital information, we refer to this scheme as digital Costa coding. We briefly review this here to make it easier to describe our proposed techniques later on. A related toy example discussing the binning schemes is described earlier in example 1.1 in section I-1.

Let U be an auxiliary random variable given by

$$U = X + \alpha S, \tag{2.4}$$

where $X \sim \mathcal{N}(0, P)$ is independent of S and $\alpha = \frac{P}{P+\sigma^2}$.

We first create an N-length i.i.d Gaussian code book $\mathcal{U}$ with $2^{N(I(U;Y)-\delta)}$ codewords, where each component of the codeword is Gaussian with zero mean and variance $P + \alpha^2 Q$. Then evenly (randomly) distribute these over 2^{NR} bins. For each $\mathbf{u}$, let $i(\mathbf{u})$ be the index of the bin containing $\mathbf{u}$. For a given m, we look for an $\mathbf{u}$ such that $i(\mathbf{u}) = m$ and $(\mathbf{u}, \mathbf{s})$ are jointly typical. Then, we transmit $\mathbf{x} = \mathbf{u} - \alpha\mathbf{s}$. Note that since $(\mathbf{u}, \mathbf{s})$ are jointly typical, from (2.4), we can see that $\mathbf{x} \perp \mathbf{s}$ and satisfies the power constraint.

The received sequence $\mathbf{y}$ is given by

$$\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w}. \tag{2.5}$$

At the decoder, we look for a $\mathbf{u}$ that is jointly typical with $\mathbf{y}$ and declare $i(\mathbf{u})$ to be the decoded message. Since $R = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right) - \epsilon$, the distortion in $\mathbf{v}$ given by $D(R)$, where D is the distortion rate function. For a Gaussian source and mean squared error distortion $D(R) = \sigma_v^2 2^{-2R}$ and, hence, the overall distortion can be made to be arbitrarily close to $\frac{\sigma_v^2}{\left(1+\frac{P}{\sigma^2}\right)}$ by a proper choice of ϵ and δ.

While the above scheme is straightforward, in the following three sections we show that there are a few other joint source-channel coding schemes, which are also optimal. In fact, there are infinitely many schemes which are optimal. Although, these schemes are all optimal when the channel SNR is known at the transmitter, their performance is in general different when there is an SNR mismatch or when the receiver is interested in estimating also the state signal $\mathbf{s}$ in addition to the source signal. The joint source channel coding schemes to be discussed in the next sections have advantages over the separation based scheme discussed in such a situation.

2. Hybrid digital analog(HDA) Costa coding

We will now describe a joint source-channel coding scheme where the source $\mathbf{v}$ is not explicitly quantized. We refer to this scheme as hybrid digital analog (HDA) Costa coding for which the code construction, encoding and decoding procedures are as described below. A rigorous proof of the achievable distortion for this scheme is given in appendix G.2. It should be noticed that all achievability results in this chapter can be proved along the same lines as in appendix G.2, using standard typicality analysis.

We first define an auxiliary random variable U given by

$$U = X + \alpha S + \kappa V, \tag{2.6}$$

where $X \sim \mathcal{N}(0, P)$ and X, S and V are pairwise independent.

1. Codebook generation: Generate a random i.i.d code book $\mathcal{U}$ with 2^{NR_1} sequences, where each component of each codeword is Gaussian with zero mean and variance $P + \alpha^2 Q + \kappa^2 \sigma_v^2$.

2. Encoding: Given an $\mathbf{s}$ and $\mathbf{v}$, find a $\mathbf{u}$ such that $(\mathbf{u}, \mathbf{s}, \mathbf{v})$ are jointly typical (see section 2 for a precise definition of typicality) with respect to the distribution obtained from the model in (2.6) and transmit $\mathbf{x} = \mathbf{u} - \alpha\mathbf{s} - \kappa\mathbf{v}$. If such an $\mathbf{u}$ cannot be found, we declare an encoder failure. Let P_{e_1} be the probability of an encoder failure.

   From standard arguments on the average performance over the ensemble of randomly generated codes, typicality and its extensions to the infinite alphabet case [12], it follows that $P_{e_1} \to 0$ as $N \to \infty$ provided

$$\begin{aligned} R_1 &> I(U; S, V) && (2.7)\\ &= h(U) - h(U|S, V) && (2.8)\\ &= h(U) - h(X|S, V) && (2.9)\\ &= h(U) - h(X) && (2.10)\\ &= \frac{1}{2} \log \frac{P + \alpha^2 Q + \kappa^2 \sigma_v^2}{P}, && (2.11) \end{aligned}$$

   where the results follow because $X = U - \alpha S - \kappa V$ and $X \perp S, V$. Notice that when a $\mathbf{u}$ that is jointly typical with $\mathbf{s}$ and $\mathbf{v}$ is found, $\mathbf{x}$ satisfies the power constraint.

3. Decoding : The received signal is $\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w}$. At the decoder, we look for an $\mathbf{u}$ that is jointly typical with $\mathbf{y}$. If such a unique $\mathbf{u}$ can be found, we declare $\mathbf{u}$ as the decoder output or, else, we declare a decoder failure. Let P_{e_2} be the probability of the event that the decoder output is not equal to the encoded $\mathbf{u}$ (this includes the probability of decoder failure as well as the probability of a decoder error).

   By using typicality arguments as discussed in appendix G.2, specifically in the evaluation of the probabilities of the events $\mathcal{E}_3$ and $\mathcal{E}_4$, and also from the extensions of typicality arguments to the infinite alphabet case [12], $P_{e_2} \to 0$ as $N \to \infty$ provided that

$$\begin{aligned} I(U;Y) &> R_1 \\ I(U;Y) &= h(U) - h(U|Y) \\ &= h(U) - h(U - \alpha Y|Y) \\ &= h(U) - h(X + \alpha S + \kappa V - \alpha X - \alpha S - \alpha W|Y) \\ &= h(U) - h(\kappa V + (1-\alpha)X - \alpha W|Y) \end{aligned} \tag{2.12}$$

   Now, let us choose

$$\alpha = \frac{P}{P+\sigma^2} \tag{2.13}$$

$$\kappa^2 = \frac{P^2}{(P+\sigma^2)\sigma_v^2} - \frac{\epsilon}{\sigma_v^2}. \tag{2.14}$$

   For the above choice of α, it can be seen that

$$\mathbb{E}[(\kappa V + (1-\alpha)X - \alpha W)Y] = 0$$

and, hence, (2.12) reduces to

$$I(U;Y) = h(U) - h(\kappa V + (1-\alpha)X - \alpha W)$$
$$= \frac{1}{2}\log\frac{P+\alpha^2 Q+\kappa^2\sigma_v^2}{P-\epsilon}. \tag{2.15}$$

Hence, P_{e_2} can be made arbitrarily small as long as

$$R_1 < \frac{1}{2}\log\frac{P+\alpha^2 Q+\kappa^2\sigma_v^2}{P-\epsilon}. \tag{2.16}$$

Combining this with the condition for encoder failure, P_{e_1} and P_{e_2} can both be made arbitrarily small provided

$$\frac{1}{2}\log\frac{P+\alpha^2 Q+\kappa^2\sigma_v^2}{P} < R_1 < \frac{1}{2}\log\frac{P+\alpha^2 Q+\kappa^2\sigma_v^2}{P-\epsilon}. \tag{2.17}$$

Therefore, by choosing an ϵ_1, $0 < \epsilon_1 < \epsilon$ and $R_1 = \frac{1}{2}\log\frac{P+\alpha^2 Q+\kappa^2\sigma_v^2}{P-\epsilon_1}$ we can satisfy (2.17) and make $P_{e_1} \to 0$ and $P_{e_2} \to 0$ as $N \to \infty$.

4. Estimation: If there is no decoding failure, we form the final estimate of $\mathbf{v}$ as an MMSE estimate of $\mathbf{v}$ from $[\mathbf{y}\ \mathbf{u}]$. After some algebra this is given by,

$$\hat{\mathbf{v}} = \frac{\kappa\sigma_v^2}{P-\epsilon}(\mathbf{u} - \alpha\mathbf{y}). \tag{2.18}$$

The distortion is then given by,

$$E[(V-\hat{V})^2] = \frac{\sigma_v^2}{1+\frac{P}{\sigma^2}}\frac{P}{P-\epsilon} \le \frac{\sigma_v^2}{1+\frac{P}{\sigma^2}} + \delta(\epsilon) \tag{2.19}$$

with $\delta(\epsilon)$ is vanishing for arbitrarily small ϵ. If an encoder or decoder failure was declared, we set the estimate of $\mathbf{v}$ to be the zero vector. However, as shown in appendix G.2 the probability of these events can be made arbitrarily small and, hence, they do not contribute to the overall distortion, which can be seen to be arbitrarily close to the optimal distortion achievable in the absence of the interference. This argument is made precise in the proof in appendix G.2.

We have presented a joint source channel coding scheme in the presence of an interference known only to the transmitter. The use of the term hybrid digital analog Costa coding needs some explanation. The scheme is not entirely analog in that it makes uses of an auxiliary codebook with a finite and discrete set of points. However, in contrast to digital Costa coding, the source is not explicitly quantized but instead is embedded into the transmitted signal $\mathbf{x}$ in an analog fashion. This is the reason for calling this as HDA Costa coding and this has some interesting consequences which are discussed in the following section.

Another feature of the HDA Costa coding scheme is that it does not make use of binning, rather it needs a single quantizer codebook that is also a good channel code. In practice, this may have some impact on the design since there are ensembles of codes that are provably good quantizers and channel codes [13]. In the Gaussian case, good lattices that are both good for coding and for quantization are known. The binning approach however, requires a nesting condition. That is, the fine code must be a good channel code, but it must contain a subcode (or a coarse code) and its cosets that must be good quantizers. This may be a more difficult condition to obtain in practice. In practical code design and finite dimension the nesting condition imposes some restriction on the "nesting ratio", that is, the binning coding rate is restricted by the lattice geometry. In our scheme, instead, we do not have such restrictions even for small N.

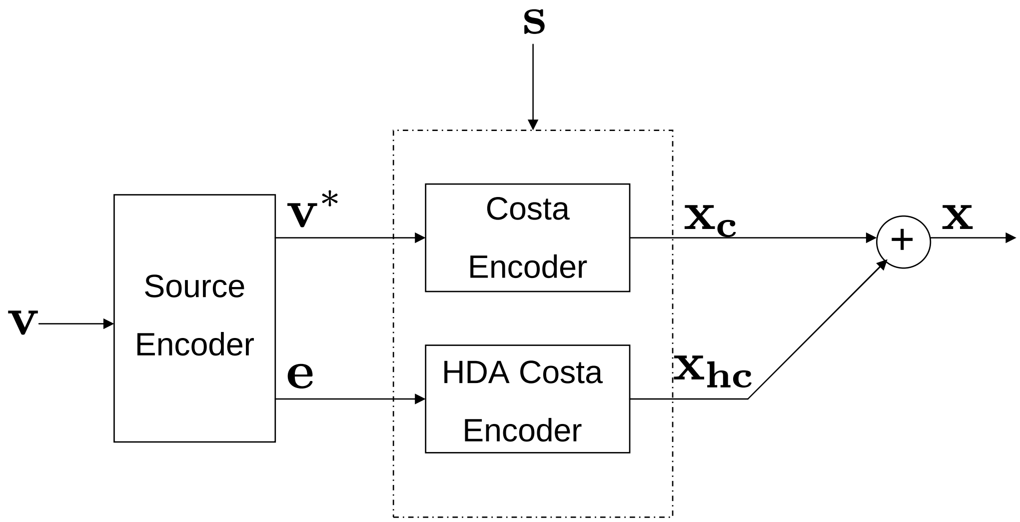

Fig. 3. Encoder model for superimposed coding.

3. Superimposed digital and HDA Costa coding scheme

Recently in [11], Bross, Lapidoth and Tinguely considered the problem of transmitting N samples of a Gaussian source in N uses of an AWGN channel, in the absence of the interferer. They showed that there are infinitely many superposition based schemes, which contain pure separation based scheme and uncoded transmission as special cases. In this section, we show that the same is true in the presence of an interference also and show the corresponding scheme, which is given in Fig. 3.

The transmitted signal is a superposition of two signals $\mathbf{x_c}$ and $\mathbf{x_{hc}}$, which are the outputs of a digital Costa encoder and an HDA encoder, respectively.

The source is first quantized at a rate of $R < C$ using an optimal source code and let the quantization error be $\mathbf{e} = \mathbf{v} - \mathbf{v}^*$, where $\mathbf{v}^*$ is the reconstruction. The quantization error $\mathbf{e}$ has a variance $\sigma_e^2 = \sigma_v^2 2^{-2R}$. The first stream in Fig. 3 is a digital Costa encoder that encodes the quantization index by treating $\mathbf{s}$ as interference and produces the signal $\mathbf{x_c}$, which has a power of P_C. The second stream is a HDA Costa encoder of rate R which treats $\mathbf{s}$ and $\mathbf{x_c}$ as interference and produces $\mathbf{x_{hc}}$, which has a power of $P_{HC} = P - P_C$. The transmitted signal is the superposition (sum) of $\mathbf{x_c}$ and $\mathbf{x_{hc}}$.

In the digital Costa encoder in the first stream, the auxiliary random variable is given by $U_c = X_c + \alpha_c S$ with $X_c \perp S$. A power of $P_C = (P + \sigma^2)(1 - 2^{-2R})$ is used in the first stream and α_c is chosen as $\frac{P_C}{P_C + P_{HC} + \sigma^2}$. Note that this corresponds to treating $\mathbf{x_{hc}}$ as noise in addition to the channel noise.

In the second stream, the quantization error $\mathbf{e}$ is encoded using an HDA Costa coding scheme and a power of $P_{HC} = P - P_C = (P + \sigma^2)2^{-2R} - \sigma^2$ is used. Note that since $R < C$, the power P_{HC} is always positive. The auxiliary random variable is chosen as $U_{hc} = X_{hc} + \alpha_{hc}(X_c + S) + \kappa E$, where $\mathbf{x_c} + \mathbf{s}$ acts as the net interference. Hence, $\mathbf{x_{hc}}$ is chosen to be independent of $\mathbf{x_c}$, $\mathbf{s}$ and $\mathbf{e}$, and α_{hc} is chosen to be $\frac{P_{HC}}{P_{HC}+\sigma^2}$. κ is chosen similar to (2.14) which gives $\kappa^2 = \frac{P_{HC}^2}{(P_{HC}+\sigma^2)\sigma_v^2 2^{-2R}} - \frac{\epsilon}{\sigma_v^2 2^{-2R}}$.

At the decoder the quantization index from the first stream is first decoded and the reconstruction $\mathbf{v}^*$ is obtained. Then, an estimate of the quantization error $\mathbf{e}$ is obtained from the second stream using the HDA costa decoder. The overall distortion is the distortion in estimating $\mathbf{e}$. Using the analysis of the HDA Costa scheme in Section 2, this can be seen to be

$$D = \frac{\sigma_e^2}{1 + \frac{(P+\sigma^2)2^{-2R} - \sigma^2}{\sigma^2}} + \delta(\epsilon) = \frac{\sigma_v^2}{1 + \frac{P}{\sigma^2}} + \delta(\epsilon). \tag{2.20}$$

By choosing ϵ to be arbitrarily small we can make $\delta(\epsilon) \to 0$ and achieve a distortion of $D = \frac{\sigma_v^2}{1+\frac{P}{\sigma^2}}$, which is the optimal distortion.

Note that for any source coding rate chosen in the first stream namely R, the resulting distortion is optimal. By varying R, we can get an infinite family of optimal joint source channel coding schemes.

4. Generalized hybrid Costa coding

In the previous section, we described a superposition technique. In this section we show a scheme that does not explicitly perform superposition. Moreover, this also introduces an interesting scheme that is an intermediate between HDA Costa having no bins to the digital Costa having bins corresponding to the capacity of the channel.

Once again we quantize the source $\mathbf{v}$ to $\mathbf{v}^*$ at a rate R, that is strictly lesser than the channel capacity, using an optimal vector quantizer. Let $\mathbf{e} = \mathbf{v} - \mathbf{v}^*$ be the quantization error vector. Note that for an optimal quantizer, as the Rate-Distortion limit is approached, the quantization error $\mathbf{e}$ will be Gaussian.

We next define an auxiliary random variable U given by

$$U = X + \alpha S + \kappa_1 E, \tag{2.21}$$

where $X \sim \mathcal{N}(0, P), E \sim \mathcal{N}(0, \sigma_v^2 2^{-2R})$, and X, S and E are independent of each other. α and κ_1 are constants, the choice of which is discussed below

1. Codebook generation: Generate a random i.i.d code book $\mathcal{U}$ with $2^{NI(U;Y)}$ sequences, where each component of each codeword is Gaussian with zero mean and variance $P + \alpha^2 Q + \kappa_1^2 \sigma_v^2 2^{-2R}$. These codewords are uniformly distributed in 2^{NR} bins and this is shared between the encoder and the decoder.

2. Encoding: Let m be the quantization index corresponding to the quantized source $\mathbf{v}^*$. Let $i(\mathbf{u})$ represent the index of a bin that contains $\mathbf{u}$. For a given m find an $\mathbf{u}$ such that $i(\mathbf{u}) = m$ and $(\mathbf{u}, \mathbf{s}, \mathbf{e})$ are jointly typical with respect to the distribution in model (2.21). We then transmit the vector $\mathbf{x} = \mathbf{u} - \alpha \mathbf{s} - \kappa_1 \mathbf{e}$. Note that since $(\mathbf{u}, \mathbf{s}, \mathbf{e})$ are jointly typical, from (2.21), we can see that $\mathbf{x} \perp \mathbf{s}, \mathbf{e}$ and satisfies the power constraint.

3. Decoding : The received signal is $\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w}$. At the decoder, we look for an $\mathbf{u}$ that is jointly typical with $\mathbf{y}$. If such a unique $\mathbf{u}$ can be found, we declare $\mathbf{u}$ as the decoder output or, else, we declare a decoder failure. Next we make an estimate of $\mathbf{e}$ from $\mathbf{u}$ and $\mathbf{y}$.

   We can see by similar Gelfand-Pinsker coding arguments that $R < I(U;Y) - I(U;S,E)$. Note

$$\begin{aligned} I(U;Y) - I(U;S,E) & \\ &= h(U|S,E) - h(U|Y) \\ &= h(X) - h(U - \alpha Y|Y) \\ &= h(X) - h(\kappa_1 E + (1-\alpha)X - \alpha W|Y) \\ &\overset{(a)}{=} h(X) - h(\kappa_1 E + (1-\alpha)X - \alpha W) \\ &= \frac{1}{2}\log\left(\frac{P}{\kappa_1^2\sigma_v^2 2^{-2R} + (1-\alpha)^2 P + \alpha^2\sigma^2}\right) \\ &\overset{(b)}{>} R. \end{aligned} \tag{2.22}$$

   In (2.22) we choose $\alpha = \frac{P}{P+\sigma^2}$ and $\kappa_1^2 = \frac{P}{P+\sigma^2}\frac{(P+\sigma^2)-\sigma^2 2^{2R}}{\sigma_v^2} - \frac{\epsilon((P+\sigma^2)-\sigma^2 2^{2R})}{P\sigma_v^2}$. The choice of α ensures $(1-\alpha)X - \alpha W$ is orthogonal to Y to get the equality in (a). κ_1 is chosen as above to satisfy the inequality in (b). This shows that we can decode the codeword $\mathbf{u}$ with a very high probability and we can decode the message $m = i(\mathbf{u})$ and $\mathbf{v}^*$.

4. Estimation: If there is no decoding failure, we form the final estimate of $\mathbf{v}$ as an MMSE estimate of $\mathbf{v}$ from $[\mathbf{v}^*\ \mathbf{u}\ \mathbf{y}]$. The estimate can be obtained as follows. Let us define $\sigma_e^2 = \sigma_v^2 2^{-2R}$. Let $\mathbf{\Lambda}$ be the covariance matrix of $[V^*\ U\ Y]^T$ and let $\mathbf{\Gamma}$ be the correlation vector between V and $[V^*\ U\ Y]^T$. Then, $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ are

given by

$$\mathbf{\Lambda} = \begin{pmatrix} \sigma_v^2 - \sigma_e^2 & 0 & 0 \\ 0 & P + \kappa_1^2\sigma_e^2 + \alpha^2 Q & P + \alpha Q \\ 0 & P + \alpha Q & P + Q + \sigma^2 \end{pmatrix}$$

$$\text{and } \mathbf{\Gamma} = \begin{pmatrix} \sigma_v^2 - \sigma_e^2 & \kappa_1\sigma_e^2 & 0 \end{pmatrix}^T.$$

The coefficients of the linear MMSE estimate are given by $\mathbf{\Lambda^{-1}\Gamma}$ and the minimum mean-squared error is given by

$$D = \sigma_v^2 - \mathbf{\Gamma}^T\mathbf{\Lambda^{-1}\Gamma} = \left(\frac{\sigma_v^2}{1 + \frac{P}{\sigma^2}}\right) + \delta(\epsilon),$$

where $\delta(\epsilon) \to 0$ as $\epsilon \to 0$. Thus, in the limit of $\epsilon \to 0$, $D = \left(\frac{\sigma_v^2}{1+\frac{P}{\sigma^2}}\right)$.

It must be noted that this scheme is an intermediate between digital Costa coding scheme with the maximum possible bins equal to the capacity of the channel and the HDA Costa coding scheme with no bins. Thus we can get a family of schemes with varying bins for the Gaussian channel.

The generalized hybrid Costa coding scheme appears to be closely related to the superimposed digital and HDA Costa coding schemes. The subtle difference however is in the generalized hybrid Costa coding scheme, the transmitted signal X is not a superposition of two streams as seen in the superposition case.

One may wonder whether there is any benefit in using the superimposed digital and HDA Costa coding scheme in section B.3 or the generalized HDA Costa coding scheme. Even though all these schemes are optimal when the channel SNR is known at the transmitter, their performances are different when the channel SNR is not known at the transmitter. Further, sometimes we are interested not only in estimating the source but also in estimating the interference. In this case also, the performance of these schemes is different. This has applications in designing schemes for broadcasting a source with bandwidth compression which is discussed in chapter III-C. In these cases, the performance of the superimposed digital and HDA Costa is different from that of just the HDA Costa coding scheme and, hence, the superimposed scheme is useful in building schemes for such applications. This is described in detail in the later sections.

C. JSCC for source side information available at the receiver

In this section, we consider the problem of transmitting a discrete-time analog source over a Gaussian noise channel when the receiver has some side information about the source. This problem is a dual of the problem considered in the previous section and is considered here for the sake of completeness. Consider the system model as shown in Fig. 4. Let $\mathbf{v} \in \mathbb{R}^N$ be the discrete-time analog source where V's are independent

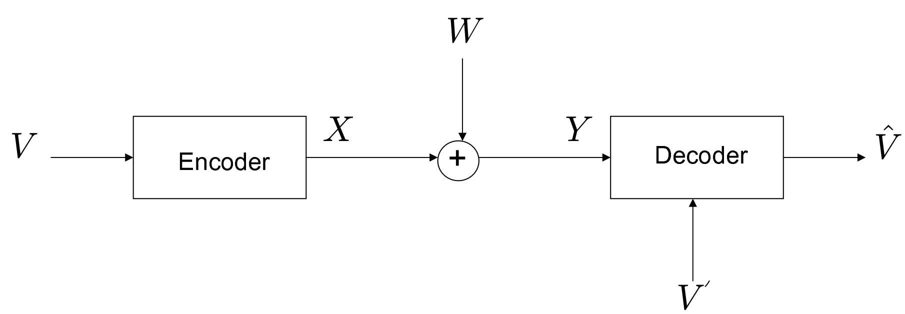

Fig. 4. Block diagram of the joint source channel coding problem with source side information known only at the receiver.

Gaussian random variables with $V \sim \mathcal{N}(0, \sigma_v^2)$. Let $\mathbf{v}' \in \mathbb{R}^N$ be the side information that is known only at the receiver. The correlation between the source and the side information is modeled as

$$V = V' + Z, \tag{2.23}$$

where $Z \sim \mathcal{N}(0, \sigma_z^2)$ and V' is i.i.d Gaussian. Here V' and Z are mutually independent random variables. The source $\mathbf{v}$ must be encoded into $\mathbf{x}$ and transmitted over an AWGN channel and the received signal is

$$\mathbf{y} = \mathbf{x} + \mathbf{w}, \tag{2.24}$$

where $\mathbf{x}$ satisfies a power constraint P and $\mathbf{w}$ is AWGN having a noise variance of σ^2. The following schemes can be shown to be optimal for this case.

1. Separation based scheme with Wyner-Ziv coding (digital Wyner-Ziv coding)

One strategy is using a separation scheme with an optimal Wyner-Ziv code of rate R followed by a channel code. We also refer to this scheme as the digital Wyner-Ziv scheme. We briefly explain the digital Wyner-Ziv scheme and then establish our information theoretic model for the HDA Wyner-Ziv coding scheme.

Suppose the source side information is available both at the encoder as well as the receiver, the best possible distortion is $D = \frac{\sigma_z^2}{1+\frac{P}{\sigma^2}}$. The same distortion can be achieved using the following scheme and is a direct consequence of Wyner and Ziv's result [14]. This can be achieved as follows,

Let U be an auxiliary random variable given by

$$U = \sqrt{\alpha} V + B, \tag{2.25}$$

where $\alpha = 1 - \frac{D}{\sigma_z^2} = \frac{P}{P+\sigma^2}$ and $B \sim \mathcal{N}(0, D)$. We create an N-length i.i.d Gaussian code book $\mathcal{U}$ with $2^{NI(U;V)}$ codewords, where each component of the codeword is Gaussian with zero mean and variance $\alpha\sigma_v^2 + D$ and evenly distribute them over 2^{NR}

bins. Let $i(\mathbf{u})$ be the index of the bin containing $\mathbf{u}$. For each $\mathbf{v}$, find an $\mathbf{u}$ such that $(\mathbf{u}, \mathbf{v})$ are jointly typical. The index $i(\mathbf{u})$ is the Wyner-Ziv source coded index. The index $i(\mathbf{u})$ is encoded using an optimal channel code of rate arbitrarily close to $\frac{1}{2}\log(1+\frac{P}{\sigma^2})$ and transmitted over the channel. At the receiver decoding of the index $i(\mathbf{u})$ is possible with high probability as an optimal code book for the channel is used. Next for the decoded $i(\mathbf{u})$ we look for an $\mathbf{u}$ in the bin whose index is $i(\mathbf{u})$ such that $(\mathbf{u}, \mathbf{v}')$ are jointly typical. From $\mathbf{v}'$ and the decoded $\mathbf{u}$ we make an estimate of the source $\mathbf{v}$ as follows.

$$\hat{\mathbf{v}} = \mathbf{v}' + \sqrt{\alpha}(\mathbf{u} - \sqrt{\alpha}\mathbf{v}') \tag{2.26}$$

This yields the optimal distortion D.

2. Hybrid digital analog Wyner-Ziv coding

In this section, we discuss a different joint source channel coding scheme that does not involve quantizing the source explicitly. This scheme is quite similar to the modulo lattice modulation scheme in [15]; the difference being that a nested lattice is not used. The auxiliary random variable U is generated as follows.

$$U = X + \kappa V, \tag{2.27}$$

where κ is defined as $\kappa^2 = \frac{P^2}{(P+\sigma^2)\sigma_z^2} - \frac{\epsilon}{\sigma_z^2}$ and $X \sim \mathcal{N}(0, P)$.

1. Codebook generation: Generate a random i.i.d code book $\mathcal{U}$ with 2^{NR_1} sequences, where each component of each codeword is Gaussian with zero mean and variance $P + \kappa^2\sigma_v^2$. This codebook is shared between the encoder and the decoder.

2. Encoding: For a given $\mathbf{v}$ find an $\mathbf{u}$ such that $(\mathbf{u}, \mathbf{v})$ are jointly typical and transmit $\mathbf{x} = \mathbf{u} - \kappa\mathbf{v}$. This is possible with arbitrarily high probability if

$R_1 > I(U;V)$.

3. Decoding: The received signal is $\mathbf{y} = \mathbf{x} + \mathbf{w}$. Find an $\mathbf{u}$ such that $(\mathbf{v}', \mathbf{y}, \mathbf{u})$ are jointly typical. A unique such $\mathbf{u}$ can be found with arbitrarily high probability if $R_1 < I(U;V',Y)$. We next show below that we can choose an R_1 to satisfy $I(U;V) < R_1 < I(U;V',Y)$. This requires $I(U;V) < I(U;V',Y)$ which can be shown as follows,

$$\begin{aligned}
I(U;V',Y) &= h(U) - h(U|V',Y) \\
&= h(U) - h(U - \kappa V' - \alpha Y | V', Y) \\
&= h(U) - h(\kappa Z + (1-\alpha)X - \alpha W | V', Y) \\
&\overset{(a)}{=} h(U) - h(\kappa Z + (1-\alpha)X - \alpha W) \\
&= \frac{1}{2}\log\left(\frac{P + \kappa^2\sigma_v^2}{\kappa^2\sigma_z^2 + (1-\alpha)^2 P + \alpha^2\sigma^2}\right) \\
&\overset{(b)}{=} \frac{1}{2}\log\left(\frac{P + \kappa^2\sigma_v^2}{P}\right) + \delta(\epsilon) \\
&= h(U) - h(U|V) + \delta(\epsilon) \\
&= I(U;V) + \delta(\epsilon). \qquad (2.28)
\end{aligned}$$

In (2.28), (a) follows because $(\kappa Z + (1-\alpha)X - \alpha W)$ is independent of Y and V'. (b) follows because we can always find a $\delta(\epsilon) > 0$ for the choice of $\kappa^2 = \frac{P^2}{(P+\sigma^2)\sigma_z^2} - \frac{\epsilon}{\sigma_z^2}$. Hence from knowing $\mathbf{v}'$, $\mathbf{u}$ and $\mathbf{y}$ we can make an estimate of $\mathbf{v}$. Since all random variables are Gaussian, the optimal estimate is a linear MMSE estimate which can be computed as follows.

Let $\mathbf{\Lambda}$ be the covariance matrix of $[V' \; U \; Y]^T$ and let $\mathbf{\Gamma}$ be the correlation between V and $[V' \; U \; Y]^T$. $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ are given by

$$\mathbf{\Lambda} = \begin{pmatrix} \sigma_v^2 - \sigma_z^2 & \kappa(\sigma_v^2 - \sigma_z^2) & 0 \\ \kappa(\sigma_v^2 - \sigma_z^2) & P + \kappa^2\sigma_v^2 & P \\ 0 & P & P + \sigma^2 \end{pmatrix} \text{ and } \mathbf{\Gamma} = \begin{pmatrix} \sigma_v^2 - \sigma_z^2 & \kappa\sigma_v^2 & 0 \end{pmatrix}^T.$$

The coefficients of the linear MMSE estimate are given by $\mathbf{\Lambda^{-1}\Gamma}$ and this yields the optimal MMSE estimate which is given below as,

$$\hat{\mathbf{v}} = \mathbf{v}' + \frac{\kappa\sigma_z^2}{P}(\mathbf{u} - \kappa\mathbf{v}' - \alpha\mathbf{y}). \tag{2.29}$$

The distortion D is given by

$$\begin{aligned} D &= E[(\mathbf{v} - \hat{\mathbf{v}})^2] \\ &= E[(\mathbf{v} - \mathbf{v}' - \frac{\kappa\sigma_z^2}{P}(\mathbf{u} - \kappa\mathbf{v}' - \alpha\mathbf{y}))^2] \\ &= E[(\mathbf{z} - \frac{\kappa\sigma_z^2}{P}(\kappa\mathbf{z} + \mathbf{x} - \alpha\mathbf{y}))^2] \\ &= E[((1 - \frac{\kappa^2\sigma_z^2}{P})\mathbf{z} - \frac{\kappa\sigma_z^2}{P}((1-\alpha)\mathbf{x} - \alpha\mathbf{w}))^2] \\ &\overset{(a)}{=} \frac{\sigma_z^2}{1 + \frac{P}{\sigma^2}} + \delta(\epsilon). \end{aligned} \tag{2.30}$$

Here, (a) follows by using the appropriate values of κ and α. We once again obtain the optimal distortion D by making ϵ arbitrarily small and $\delta(\epsilon) \to 0$.

It is instructive to compare the performance of this scheme with that of the following naive scheme that would be optimal in the absence of side-information at the receiver. In the naive scheme, the $\mathbf{v}$ is transmitted directly (analog transmission). At the receiver, an MMSE estimate of $\mathbf{v}$ is formed from the received signal $\mathbf{y}$ and the available source side information $\mathbf{v}'$. The distortion for this naive scheme can be seen to be $D_{naive} = \frac{\sigma_z^2}{1+\frac{P}{\sigma^2}\frac{\sigma_z^2}{\sigma_v^2}}$.

Notice that $\frac{\partial D_{naive}}{\partial \sigma_z^2}|_{\sigma_z^2=0} = 1$, whereas for the Wyner-Ziv scheme, $\frac{\partial D}{\partial \sigma_z^2}|_{\sigma_z^2=0} = \frac{1}{1+P/\sigma^2} < 1$. At $\sigma_z^2 = 0$, both D_{naive} and D are zero. i.e., the optimal scheme and the naive scheme approach zero distortion with different slopes.

Similarly, in the absence of any side information which corresponds to $\sigma_z^2 = \sigma_v^2$, both the naive scheme and the Wyner-Ziv scheme are optimal. Again, the two schemes approach the optimal distortion with different slopes.

$$\left.\frac{\partial D_{naive}}{\partial \sigma_z^2}\right|_{\sigma_z^2=\sigma_v^2} = \frac{1}{(1+\frac{P}{\sigma^2})^2} < \frac{1}{1+\frac{P}{\sigma^2}} = \frac{\partial D_{opt}}{\partial \sigma_z^2}.$$

3. Superimposed digital and HDA Wyner-Ziv scheme

The above results could also be extended to a form of superimposed digital and analog coding. This is similar to the superimposed digital and HDA Costa coding case discussed in section B. 3. We once again have two streams as shown in Fig. 5. The first stream uses a rate R Wyner-Ziv code to quantize the source assuming the source side information $\mathbf{v}'$ is known at the receiver and the discrete index is encoded using an optimal channel code to produce the codeword $\mathbf{x}_1$. The power allocated to this stream is $P_{WZ} = (P+\sigma^2)(1-2^{-2R})$. The second stream uses the HDA Wyner-Ziv scheme and produces the output $\mathbf{x}_2$. The auxiliary random variable of the HDA scheme is given by

$$U = \kappa_1 V + X_2 \tag{2.31}$$

with $X_2 \sim \mathcal{N}(0, P_{HWZ})$, where $P_{HWZ} = (P+\sigma^2)2^{-2R} - \sigma^2$ and X_2 and V are independent. We also choose $\kappa_1^2 = \frac{P_{HWZ}^2}{(P_{HWZ}+\sigma^2)\sigma_e^2} - \frac{\epsilon}{\sigma_e^2}$ where $\sigma_e^2 = \sigma_z^2 2^{-2R}$.

The two streams ($\mathbf{x}_1$ and $\mathbf{x}_2$) are superimposed and transmitted through the channel. The received signal is given by $\mathbf{y} = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{w}$. At the receiver $\mathbf{x}_1$ is decoded assuming $\mathbf{x}_2 + \mathbf{w}$ as independent noise and this gives the Wyner-Ziv encoded bits (index). This along with the source side information $\mathbf{v}'$ can be used to make an estimate of the source $\mathbf{v}$ and we call the estimate as $\tilde{\mathbf{v}}$. The random variables corresponding to $\mathbf{v}$ and $\tilde{\mathbf{v}}$ are related as

$$V = \tilde{V} + \tilde{Z} \tag{2.32}$$

with $\tilde{Z}$ having a variance $\sigma_z^2 2^{-2R}$. When the digital part is first decoded and canceled from the received signal, we get an equivalent channel for the HDA Wyner-Ziv scheme with power constraint P_{HWZ} and channel noise σ^2. We next make a final estimate of $\mathbf{v}$ using a HDA Wyner-Ziv decoder from the new source side information $\tilde{\mathbf{v}}$, the observed equivalent channel $(\mathbf{y}-\mathbf{x}_1)$ and the decoded $\mathbf{u}$. Notice that since the choice of $\kappa_1^2 = \frac{P_{HWZ}^2}{(P_{HWZ}+\sigma^2)\sigma_e^2} - \frac{\epsilon}{\sigma_e^2}$ where $\sigma_e^2 = \sigma_z^2 2^{-2R}$ is designed for the source side information $\tilde{\mathbf{v}}$, this ensures decoding of $\mathbf{u}$ with arbitrarily high probability. The achievable distortion is then given as follows.

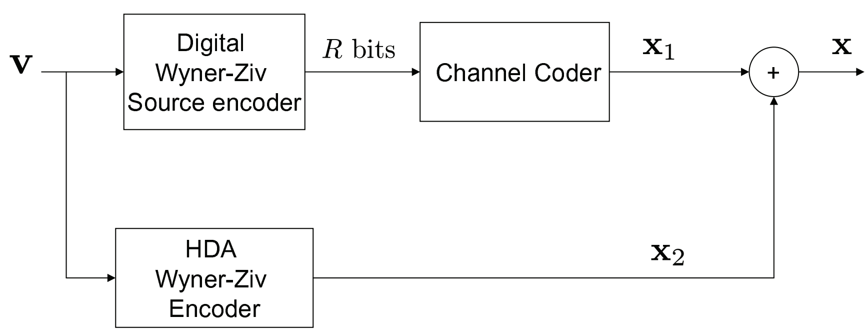

Fig. 5. Block diagram of the encoder of the superimposed digital and HDA Wyner-Ziv scheme.

$$\begin{aligned}
D &\overset{(a)}{=} \sigma_e^2 \frac{\sigma^2}{P_{HWZ}+\sigma^2} + \delta(\epsilon) \\
&= \sigma_z^2 2^{-2R} \frac{\sigma^2}{P_{HWZ}+\sigma^2} + \delta(\epsilon) \\
&\overset{(b)}{=} \sigma_z^2 \frac{P_{HWZ}+\sigma^2}{P+\sigma^2} \frac{\sigma^2}{P_{HWZ}+\sigma^2} + \delta(\epsilon) \\
&= \frac{\sigma_z^2}{1+\frac{P}{\sigma^2}} + \delta(\epsilon) \qquad (2.33)
\end{aligned}$$

Here in (2.33), (a) follows since we assume that the first stream is decoded with high probability and apply the results of HDA Wyner-Ziv decoding with the source side information $\tilde{\mathbf{v}}$. Also (b) follows since $P_{HWZ} = (P+\sigma^2)2^{-2R} - \sigma^2$. The optimal distortion $\frac{\sigma_z^2}{1+\frac{P}{\sigma^2}}$ can be obtained by making ϵ arbitrarily small and $\delta(\epsilon) \to 0$. Notice that for any rate R, $0 \le R < C$, where C is the capacity of the AWGN channel, there is a corresponding power allocation for $P_{HWZ} = (P+\sigma^2)2^{-2R} - \sigma^2$ for which the overall scheme is optimal. Thus, there are infinitely many schemes which are optimal with the digital Wyner-Ziv corresponding to $P_{HWZ} = 0$ and the HDA Wyner-Ziv corresponding to $P_{HWZ} = P$ and $R = 0$.

Further, we would like to mention that there is another way to get a family of optimal schemes using the HDA Wyner-Ziv scheme. Here, the source $\mathbf{v}$ is encoded using a HDA Wyner-Ziv encoder to the sequence $\mathbf{x}$. The auxiliary random variable U is given by

$$U = \kappa V + X \qquad (2.34)$$

where $\kappa^2 = \frac{P^2}{(P+\sigma^2)\sigma_v^2} - \frac{\epsilon}{\sigma_v^2}$. The sequence $\mathbf{x}$ can be treated as an i.i.d Gaussian source and, hence, the family of schemes proposed by Bross, Lapidoth and Tinguely [11] can be applied on $\mathbf{x}$. The scheme proposed in [11] quantizes the analog source, which in this case is $\mathbf{x}$ to a quantization index and is sent over the Gaussian channel along with the uncoded analog source (here $\mathbf{x}$) with the appropriate power scaling. At the receiver we can obtain an optimal estimate of $\mathbf{x}$ by first decoding the quantized index and then making an estimate on the analog source. Notice that the HDA Wyner-Ziv receiver only requires an optimal MMSE estimate of $\mathbf{x}$, which can be obtained using the family of schemes in [11]. Hence the resulting distortion in $\mathbf{v}$ is still optimal. To establish this claim we need to show that $\mathbf{u}$ can be decoded with arbitrarily high probability and an optimal estimate of $\mathbf{v}$ must be made using $\mathbf{u}$ and the MMSE estimate $\hat{\mathbf{x}}$.

We next show below that $I(U;V) < I(U;V',\hat{X})$. Hence, we can choose a codebook for $\mathbf{u}$ with 2^{nR_1} codewords such that $I(U;V) < R_1 < I(U;V',\hat{X})$. Since $I(U;V) < R_1$, we can find a $\mathbf{u}$ that is jointly typical with $\mathbf{v}$ with probability close to 1 and since $R_1 < I(U;V',\hat{X})$, $\mathbf{u}$ can decoded with high probability from $(\mathbf{v}',\hat{\mathbf{x}})$.

$$\begin{aligned}
I(U;V',\hat{X}) &= h(U) - h(U|V',\hat{X}) \\
&= h(U) - h(U - \kappa V' - \hat{X}|V',\hat{X}) \\
&= h(U) - h(\kappa Z + X - \hat{X}|\hat{X},V') \\
&\overset{(a)}{=} h(U) - h(\kappa Z + X - \hat{X}) \\
&\overset{(b)}{=} \frac{1}{2}\log\left(\frac{P+\kappa^2\sigma_v^2}{\kappa^2\sigma_z^2+\alpha\sigma^2}\right) \\
&= \frac{1}{2}\log\left(\frac{P+\kappa^2\sigma_v^2}{P}\right) + \delta(\epsilon) \\
&= h(U) - h(U|V) + \delta(\epsilon) \\
&= I(U;V) + \delta(\epsilon).
\end{aligned} \tag{2.35}$$

In (2.35), (a) follows because $(X-\hat{X})$ is orthogonal to $\hat{X}$ and hence $(\kappa Z + X - \hat{X})$ is independent of $\hat{X}$ and V', (b) follows because $X-\hat{X}$ is Gaussian with variance $\alpha\sigma^2$ and is orthogonal to Z. The estimate of $\mathbf{v}$ is then given by

$$\hat{\mathbf{v}} = \mathbf{v}' + \frac{\kappa\sigma_z^2}{P}(\mathbf{u} - \kappa\mathbf{v}' - \hat{\mathbf{x}}). \tag{2.36}$$

The resulting distortion can be obtained by following the steps similar to those in (2.30) which can be found to be optimal.

D. JSCC for interference known at the transmitter and source side information available at the receiver

In this section, we consider the problem of transmitting a Gaussian source $\mathbf{v}$ through an AWGN channel with channel noise variance σ^2 in the presence of an interference $\mathbf{s}$ known only at the transmitter and in the presence of source side information $\mathbf{v}'$ known only at the receiver. The source side information $\mathbf{v}'$ is assumed to be related to the source $\mathbf{v}$ according to

$$V = V' + Z,$$

where $Z \sim \mathcal{N}(0, \sigma_z^2)$ and is independent of V'.

A similar model has been considered by Merhav and Shamai [16] for a more general setup where the source and side information are not assumed to be Gaussian. They show that a separation based approach of Wyner-Ziv coding followed by Gelfand-Pinsker coding is optimal. Here, we propose a joint-source channel coding scheme when the source and channel noise are Gaussian. The proposed scheme is easily obtained by combining the results from the previous two sections. It must be noted that a similar joint source channel coding scheme using lattices and dither has been shown in [10]. However, our scheme is based on random codes.

To establish our scheme we can combine the results from the previous two sections as follows. Choose the auxiliary random variable U such that

$$U = X + \alpha S + \kappa V \tag{2.37}$$

with $\kappa^2 = \frac{P^2}{(P+\sigma^2)\sigma_z^2} - \frac{\epsilon}{\sigma_z^2}$ and $\alpha = \frac{P}{P+\sigma^2}$. Further, let $X \sim \mathcal{N}(0, P)$, $S \sim \mathcal{N}(0, Q)$

and $V \sim \mathcal{N}(0, \sigma_v^2)$ and let X, S and V be pairwise independent. A codebook $\mathcal{U}$ is obtained by generating 2^{nR_1} code sequences for $\mathbf{u}$ and this is shared between the encoder and decoder. At the encoder, the source $\mathbf{v}$ is encoded by choosing an $\mathbf{x}$ that is jointly typical with $\mathbf{u}$,$\mathbf{v}$ and $\mathbf{s}$. Such a $\mathbf{u}$ exists with high probability if we have chosen $R_1 > I(U; S, V)$. Now $\mathbf{x}$ is transmitted over the channel. The received signal vector $\mathbf{y}$ is given as

$$\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{w}.$$

At the decoder, $\mathbf{u}$ is decoded by looking for a $\mathbf{u}$ that is jointly typical with $\mathbf{y}$ and the source side information $\mathbf{v}'$. Using standard arguments on joint-typicality, it can be seen that a unique such $\mathbf{u}$ exists with high probability if $R_1 < I(U; Y, V')$. We now show that $I(U; S, V) < I(U; Y, V')$. This implies that there exists an R_1, such that $I(U; S, V) < R_1 < I(U; Y, V')$ which satisfies the requirements at the encoder and the decoder.

$$\begin{aligned}
I(U; Y, V') &= h(U) - h(U|Y, V') \\
&= h(U) - h(U - \alpha Y - \kappa V'|Y, V') \\
&= h(U) - h(\kappa Z + (1-\alpha)X - \alpha W|Y, V') \\
&\overset{(a)}{=} h(U) - h(\kappa Z + (1-\alpha)X - \alpha W) \\
&= \frac{1}{2}\log(\frac{P + \alpha^2 Q + \kappa^2\sigma_v^2}{P}) + \delta(\epsilon) \\
&= I(U; S, V) + \delta(\epsilon), \qquad (2.38)
\end{aligned}$$

where (a) follows since $\kappa Z + (1-\alpha)X - \alpha W$ is orthogonal to Y and V'. Then an optimal linear MMSE estimate of $\mathbf{v}$ is formed from the source side information $\mathbf{v}'$, the received vector $\mathbf{y}$ and the vector $\mathbf{u}$. By using the argument as in section 2, the

MMSE estimate is given by

$$\hat{\mathbf{v}} = \mathbf{v}' + \frac{\kappa\sigma_z^2}{P}(\mathbf{u} - \kappa\mathbf{v}' - \alpha\mathbf{y}). \tag{2.39}$$

The resulting distortion can be obtained by following steps similar to (2.30) and can be seen to be $D = \frac{\sigma_z^2}{1+\frac{P}{\sigma^2}}$, which is the optimal distortion.

E. Analysis of the schemes for SNR mismatch

In this section, we consider the performance of the above JSCC schemes for the case of SNR mismatch where we design the scheme to be optimal for a channel noise variance of σ^2, but the actual noise variance is σ_a^2.

Separation based digital schemes suffer from a pronounced threshold effect. When the channel SNR is worse than the designed SNR, the index cannot be decoded and when the channel SNR is better than the designed SNR, the distortion is limited by the quantization and does not improve. However, the hybrid digital analog schemes considered offer better performance in this situation.

Let us consider the joint source channel coding setup with side information at both the transmitter and receiver and $\sigma_a^2 < \sigma^2$. We can decode $\mathbf{u}$ at the receiver when the SNR is better than the designed SNR and make an estimate of the source from the various observations at the receiver as shown below.

$$U = X + \alpha S + \kappa_w V \tag{2.40}$$

$$V = V' + Z \tag{2.41}$$

$$Y = X + S + W_a, \tag{2.42}$$

where $\kappa_w = \sqrt{\frac{P^2}{(P+\sigma^2)\sigma_z^2}}$, $\alpha = \frac{P}{P+\sigma^2}$, $S \sim \mathcal{N}(0, Q)$ and $Z \sim \mathcal{N}(0, \sigma_z^2)$. From now on, we drop the ϵ's in κ_w to improve clarity. Note that α depends only on the assumed

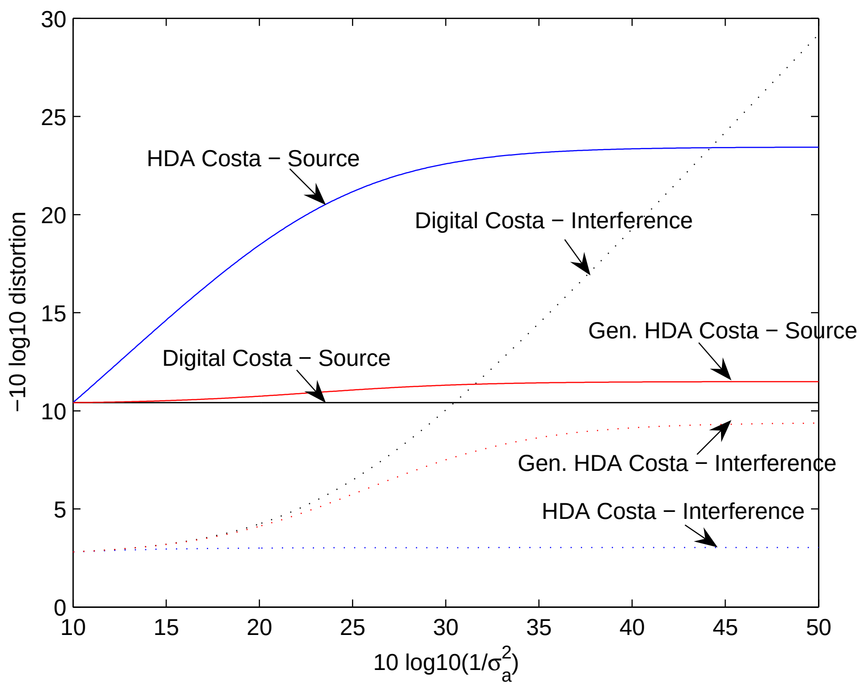

Fig. 6. Performance of the different Costa coding schemes for the joint source channel coding problem.

noise variance σ^2 and not on σ_a^2.

From the observations $[V', U, Y]$, an optimal linear MMSE estimate of V is obtained. Similar to the definition in section 2 let $\mathbf{\Lambda}$ be the covariance of $[V', U, Y]^T$ and $\mathbf{\Gamma}$ be the correlation between V and $[V', U, Y]^T$.

Hence

$$\mathbf{\Lambda} = \begin{pmatrix} \sigma_v^2 - \sigma_z^2 & \kappa(\sigma_v^2 - \sigma_z^2) & 0 \\ \kappa(\sigma_v^2 - \sigma_z^2) & P + \alpha^2 Q + \kappa_w^2 \sigma_v^2 & P + \alpha Q \\ 0 & P + \alpha Q & P + Q + \sigma_a^2 \end{pmatrix}$$

$$\text{and } \mathbf{\Gamma} = \begin{pmatrix} \sigma_v^2 - \sigma_z^2 & \kappa\sigma_v^2 & 0 \end{pmatrix}^T.$$

Then the distortion (in the presence of mismatch) is given by

$$D_a = \sigma_v^2 - \mathbf{\Gamma}^T \mathbf{\Lambda}^{-1} \mathbf{\Gamma}. \tag{2.43}$$

This on further simplification yields

$$\begin{aligned} D_a = &\left[(Q\sigma^4 + (P(P+Q) + 2P\sigma^2 + \sigma^4)\sigma_a^2)\sigma_z^2\right] \times \\ &\left[P^2(P+Q) + P(P+Q)\sigma^2 + Q\sigma^4 + (P(2P+Q) + 3P\sigma^2 + \sigma^4)\sigma_a^2\right]^{-1}. \end{aligned} \tag{2.44}$$

We will now look at a few special cases.

1. Hybrid digital analog Costa coding

In this setup there is side information only at the transmitter. The distortion achievable for the user under SNR mismatch with the actual SNR greater than the designed SNR is obtained by setting $\sigma_v = \sigma_z$ (2.44) and is given below as

$$\begin{aligned} D_{va} = &\left[(Q\sigma^4 + (P(P+Q) + 2P\sigma^2 + \sigma^4)\sigma_a^2)\sigma_v^2\right] \times \\ &\left[P^2(P+Q) + P(P+Q)\sigma^2 + Q\sigma^4 + (P(2P+Q) + 3P\sigma^2 + \sigma^4)\sigma_a^2\right]^{-1}. \end{aligned} \tag{2.45}$$

The distortion in the source $\mathbf{v}$ is shown in Fig. 6 for a designed SNR of 10 dB as the actual channel SNR ($10 \log 1/\sigma_a^2$) varies when the source and interference both have unit variance. It can be seen that the distortion in the source is smaller with the HDA Costa scheme than with the digital Costa scheme.

In some cases, the distortion in estimating the interference at the receiver may also be of interest and can be obtained by estimating S from (2.40) and (2.42). The distortion is given below as

$$\begin{aligned} D_{sa} = &\left[Q(P+\sigma^2)(P^2+(2P+\sigma^2)\sigma_a^2)\right]\times \\ &\left[P^2(P+Q)+P(P+Q)\sigma^2+Q\sigma^4(P(2P+Q)+3P\sigma^2+\sigma^4)\sigma_a^2\right]^{-1}. \end{aligned} \tag{2.46}$$

It can be seen from Fig. 6 that the distortion in estimating the interference is better for the digital scheme than for the HDA Costa scheme.

In [17], Sutivong *et al.* have studied a somewhat related problem. They consider the transmission of a digital source in the presence of an interference known at the transmitter with a fixed channel SNR. They study the optimal tradeoff between the achievable rate and the error in estimating the interference at the designed SNR. The main result is that we can get a better estimate of the interference if we transmit the digital source at a rate lesser than the channel capacity. There are important differences between our work and that in [17]. First of all, we consider transmission of an analog source instead of a digital source. Secondly, we consider mismatch in the channel, i.e., our schemes are designed to be optimal at the designed SNR and as we move away from the designed SNR, we study the tradeoff between the error in estimating the interference and the distortion in the reconstruction of the analog source. This tradeoff is discussed below.

2. Generalized HDA Costa coding under channel mismatch

Next we analyze the performance of the generalized HDA Costa coding under channel mismatch. This case leads to some interesting analysis. By changing the source coding rate of the digital part R, we can tradeoff the distortion between the source and the interference in the presence of mismatch.

The different random variables and their relations are given below.

$$U = X + \alpha S + \kappa_1 E \tag{2.47}$$

$$Y = X + S + W_a \tag{2.48}$$

$$V = V^* + E \tag{2.49}$$

In the above equation $\kappa_1 = \sqrt{\frac{P}{P+\sigma^2}\frac{(P+\sigma^2)-\sigma^2 2^{2R}}{\sigma_v^2}}$ (Again, we have dropped the ϵ in the expression for κ_1). From the above equations an estimate of S as well as V is obtained by taking a linear MMSE estimate as all the random variables are Gaussian. The resulting expressions of estimation error $D_{sa}(R)$ and $D_{va}(R)$ are given by

$$\begin{aligned} D_{va}(R) = &\left[(\sigma_a^2(\sigma^2+P)^2 + (\sigma^4 + \sigma_a^2 P)Q)\sigma_v^2\right]\times \\ &\left[(\sigma^2+P)^2(\sigma_a^2+P+Q) - 2^{2R}(\sigma^2-\sigma_a^2)P(\sigma^2+P+Q)\right]^{-1} \end{aligned} \tag{2.50}$$

$$\begin{aligned} D_{sa}(R) = &\left[(\sigma^2+P)(2^{2R}(\sigma^2-\sigma_a^2)P - (\sigma^2+P)(\sigma_a^2+P))Q\right] \\ &\times\left[2^{2R}(\sigma^2-\sigma_a^2)P(\sigma^2+P+Q) - (\sigma^2+P)^2(\sigma_a^2+P+Q)\right]^{-1}. \end{aligned} \tag{2.51}$$

The performance of the generalized HDA Costa scheme and HDA Costa scheme in relation to digital scheme is shown in Fig. 6. For example in separation using digital

Costa there is no improvement in our estimate of the analog source, but we get a better estimate of the interference as shown in Fig. 6. On the contrary for the HDA Costa scheme there is only a small improvement in the estimate of the interference but a good improvement in the estimate of the analog source. The generalized HDA Costa scheme also shows a difference in the estimate for the source and the interference for different rates R and performs as a digital Costa for the choice of $R = C$ and as a HDA Costa for the choice of $R = 0$.

The main motivation for studying these different schemes is that in some applications we are interested in estimating the interference as well as the source. For example, in the broadcasting with bandwidth compression presented in Section III-C, we split the source into two streams and one of the streams acts as interference to the other stream. In this case, we are interested in estimating both streams. The schemes considered in this section can in effect, provide a tradeoff between the estimation error in estimating the interference versus estimating the source when there is a channel mismatch. This provides the intuition to build schemes for broadcasting with bandwidth compression.

3. Hybrid digital analog Wyner-Ziv

In this case the distortion could be obtained by setting $Q = 0$ in (2.44). The actual distortion is given by

$$D_a = \frac{(P+\sigma^2)\sigma_a^2\sigma_z^2}{P^2 + (2P+\sigma^2)\sigma_a^2} \tag{2.52}$$

This is clearly better than $\frac{\sigma_z^2\sigma^2}{P+\sigma^2}$ which is what is achievable with a separation based approach. However, we do not know if this is the optimal distortion that is achievable in the presence of channel mismatch. A simple lower bound on the

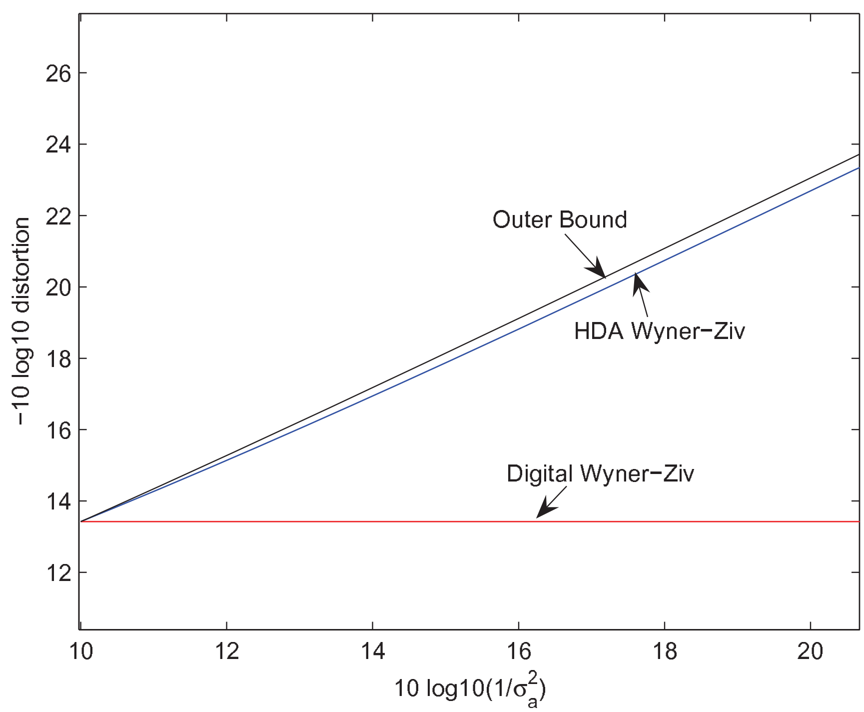

Fig. 7. Performance of the different Wyner-Ziv schemes for the joint source channel coding problem.

achievable distortion in the presence of mismatch is to assume that the transmitter knows the channel SNR. It can be seen from Fig. 7, that the performance of the HDA Wyner-Ziv scheme is very close to the outer bound.

F. Concluding remarks

In this chapter we discussed hybrid digital analog versions of Costa coding and Wyner-Ziv coding for transmitting an analog Gaussian source through an AWGN channel in the presence of an interferer known only to the transmitter and side information about the source available only to the receiver, respectively. These schemes are closely related to the schemes by Reznic, Feder and Zamir [15] and Kochman and Zamir [10] which use hybrid digital analog schemes based on lattices. However, our proposed scheme uses random codes instead of lattices used in [15] and [10]. We also showed that there are infinitely many schemes that are optimal for this problem, extending the work of Bross, Lapidoth and Tinguely [11] to the side information case. The HDA coding schemes have advantages over strictly digital schemes when there is a mismatch in the channel SNR. We also evaluated the distortion exponents of these schemes and showed that the proposed schemes provide a graceful degradation of distortion with channel SNR. Finally we presented HDA coding schemes for general discrete memoryless sources and channels, in addition to purely Gaussian source and Gaussian channels.

G. Appendix

1. Background on binning schemes

In this section, we provide some basic background on the binning schemes considered in this dissertation. We use some simple toy examples to convey the main ideas on binning. Readers familiar with Gelfand-Pinsker coding, Slepian-Wolf coding and Wyner-Ziv coding can skip this section.

Since the introduction of information theory by Shannon [2] for the discrete memoryless channel, there has been a lot of interesting work on extending the results to different communication scenarios. One such scenario is the transmission of information in the presence of interference known only at the transmitter. Such a scenario can occur in practice, when it is possible to get a very good estimate of the interference at the transmitter. Tomlinson and Harashima [18, 19] introduced pre-coding for this problem for a simple case. Gelfand and Pinsker [20] introduced random binning arguments for the above problem and obtained the capacity for the above problem. Costa in [9] showed that for the Gaussian case, using Gelfand-Pinsker coding, it is possible to obtain the same capacity of the channel as when the interference was absent. Gelfand-Pinsker coding applied to the Gaussian case is also known as "Dirty Paper" coding. We would next like to present a simple toy example to understand the coding scheme for interference known only at the transmitter.

Example 1.1 (Interference at transmitter). *Say for example there is a noiseless channel which can take only the integers* 1 *or* 0 *as input. The capacity of this channel is* 1 *bit per channel use. However, there is also an interference* s *in the channel, which is an integer from (say)* 0 *to* 127*. This interference is assumed to be known at the transmitter but unknown at the receiver. The receiver observes the integer sum of* s *and the transmitted signal. We would like to establish whether it is still possible to transmit one bit of information, even in the presence of the interference.*

A naive approach of simply mapping the information bits(say) $\{yes, no\}$ *to a* 1 *or a* 0*, as* $yes \rightarrow 1$ *and* $no \rightarrow 0$ *will fail in the presence of this integer interference. This is because the interference is very high compared to the transmitted signal and* *will completely confuse the receiver. However, we can still communicate* 1 *bit of information by mapping the information bits to an even number or an odd number, and transmitting a* 1 *or a* 0 *based on the interference in the channel. Hence for an yes, the integer* $\{(s) \mod 2\}$ *is transmitted and for a no, the integer* $\{(1+s) \mod 2\}$ *is transmitted. The decoder decodes to a yes or a no depending on whether the received integer is an even integer or odd integer.*

We have actually split the received space into two bins, namely the even integer bin containing the even integers and the odd integer bin containing the odd integers. The transmitter, based on the input information looks at the even bin or odd bin, and finds the integer in the bin that is closest to the interference and transmits the difference, which is either a 1 *or a* 0*.*

Hence, effectively Gelfand-Pinsker coding involves a form of binning with the input message mapped to the bin index and the encoder tries to find the closest codeword in a bin to the observed interference. The difference is transmitted into the channel and the decoder attempts to decode to the bin index.

For the case of side information known at the receiver and unknown at the transmitter a similar binning scheme can be used. Slepian and Wolf [21] solved the problem for the digital case, and Wyner and Ziv solved the problem for rate distortion with side information available only at the receiver [14]. The binning approach for the side information available only at the receiver can be explained by a simple toy example as follows.

Example 1.2 (Side information at receiver)**.** *Consider a source encoder that observes an integer* x *that can take any value from say* 0 *to* 127*. The receiver has a correlated side information of the source* y *that can take a value* x *or* $x+1$ *with equal probability. The source is kept unaware of the side information at the receiver. In this scenario* *what is the minimum number of bits the source encoder can use to express x?*

A naive scheme is to encode the observed x into 7 bits. If suppose the side information y is also available at the source, then the source can encode x with just one bit of information. The source encoder encodes the difference $y - x$ which is either 1 or 0. The decoder obtains x by subtracting the encoder output $(y - x)$ from its receiver side-information y.

However, we will present a scheme where it is possible to encode the source with just one bit of information, even though the source does not know y. The strategy is, the source observes x and transmits $x \mod 2$, i.e., transmits whether x is even or odd. The receiver from the knowledge of y and knowing that x is even or odd, decodes to y or $y - 1$. Hence it is possible to communicate x using just one bit.

Here the source is split into two bins namely the even bin and odd bin and the encoder transmits the bin index corresponding to the source. The receiver from the knowledge of the bin index and the side information y decodes to the observed x.

Hence effectively, Slepian-Wolf coding/Wyner-Ziv coding involves transmitting the bin index of the source codeword. The receiver from the knowledge of the transmitted bin index and the side information decodes the source codeword. Wyner-Ziv coding in addition involves a final estimate of the source from both the side information and the decoded source codeword.

2. HDA coding for general sources/channels

In this section, we give a detailed analysis of the achievable distortion for the HDA Costa coding scheme for general i.i.d sources and memoryless channels. Our proof approach relies on using ϵ-*letter* typical sequences, also called as strongly typical sequences and follows the treatment in [22]. To make the discussions more clear we first introduce some notation similar to [22] in this section. $P_X(\cdot)$ denotes the probability distribution of the random variable X and $P_{X|Y}(\cdot)$ denotes the probability distribution of X conditioned on Y. $\text{supp}(P_X)$ denotes the support of P_X and $|\cdot|$ is used to denote cardinality of a set. x^n (or $\mathbf{x}$) denotes an n-length sequence $x_1, x_2, \ldots, x_n$. $x^n y^n$ denotes a concatenation of sequences given by $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$. If a function $f(\cdot)$ acts component wise on a sequence (say x^n), then we denote it as $f^n(x^n)$, where $f^n(x^n)$ is also an $n-$length sequence given by $f(x_1), f(x_2), \ldots, f(x_n)$. Similarly $f^n(x^n, y^n)$ is an $n-$length sequence given by $f(x_1, y_1), f(x_2, y_2), \ldots, f(x_n, y_n)$. $N(a|x^n)$ denotes the number of occurrences of the alphabet a in the sequence x^n.

The ϵ-*letter* typical set with respect to $P_X(\cdot)$ is defined as

$$T_\epsilon^n(P_X) \triangleq \left\{ x^n : \left| \frac{1}{n} N(a|x^n) - P_X(a) \right| \leq \epsilon \cdot P_X(a), \quad \forall a \in \mathcal{X} \right\}$$

We next restate a few theorems from [22]. Let $\mu_X = \min_{x \in \text{supp}(P_X)} P_X(x)$ and define

$$\delta_\epsilon(n) = 2|\mathcal{X}| \cdot e^{-n\epsilon^2 \mu_X}.$$

It easily follows that $\delta_\epsilon(n) \to 0$ for a fixed ϵ and $n \to \infty$.

Theorem G.1. *(Theorem 1.1 from [22]) Suppose* $0 \leq \epsilon \leq \mu_X$, $x^n \in T_\epsilon^n(P_X)$, *and* X^n *is emitted by a discrete memoryless source (DMS)* $P_X(\cdot)$. *We have*

$$2^{-n(1+\epsilon)H(X)} \leq P_X^n(x^n) \leq 2^{-n(1-\epsilon)H(X)} \tag{2.53}$$

$$(1 - \delta_\epsilon(n))\, 2^{n(1-\epsilon)H(X)} \leq |T_\epsilon^n(P_X)| \leq 2^{n(1+\epsilon)H(X)} \tag{2.54}$$

$$(1 - \delta_\epsilon(n)) \leq Pr[X^n \in T_\epsilon^n(P_X)] \leq 1 \tag{2.55}$$

We will next define jointly and conditional typical sequences as in [22]. First, let $N(a, b|x^n, y^n)$ be the number of times the pair (a, b) occur in the sequence of pairs

(x_1, y_1), $(x_2, y_2), \ldots, (x_n, y_n)$. The jointly typical set with respect to $P_{XY}(\cdot)$ is defined as

$$T_\epsilon^n(P_{XY}) = \left\{ (x^n, y^n) : \left| \frac{1}{n} N(a, b|x^n, y^n) - P_{XY}(a, b) \right| \leq \epsilon \cdot P_{XY}(a, b), \right. \\ \left. \forall (a, b) \in \mathcal{X} \times \mathcal{Y} \right\}. \tag{2.56}$$

It can be easily seen that if $(x^n, y^n) \in T_\epsilon^n(P_{XY})$, then both $x^n \in T_\epsilon^n(P_X)$ and $y^n \in T_\epsilon^n(P_Y)$. We will prove this claim for one simple case and the other cases can be derived by a similar approach. For a given $(x^n, y^n) \in T_\epsilon^n(P_{XY})$, $\frac{1}{n} N(a|x^n)$ can be expressed as,

$$\frac{1}{n} N(a|x^n) = \sum_{b \in \mathcal{Y}} \frac{1}{n} N(a, b|x^n, y^n) \overset{(a)}{\leq} \sum_{b \in \mathcal{Y}} P_{XY}(a, b) + \sum_{b \in \mathcal{Y}} \epsilon P_{XY}(a, b) = P_X(a) + \epsilon P_X(a).$$

Here (a) follows from the definition of the jointly typical set $T_\epsilon^n(P_{XY})$. From the above equation we can establish that

$$\frac{1}{n} N(a|x^n) - P_X(a) \leq \epsilon P_X(a).$$

By similar arguments we can establish that

$$P_X(a) - \frac{1}{n} N(a|x^n) \leq \epsilon P_X(a),$$

and hence we can show that $x^n \in T_\epsilon^n(P_X)$.

A conditional typical set is defined as

$$T_\epsilon^n(P_{XY}|x^n) = \{ y^n : (x^n, y^n) \in T_\epsilon^n(P_{XY}) \}.$$

Further defining $\mu_{XY} = \min_{(a,b) \in \text{supp}(P_{XY})} P_{XY}(a, b)$ and

$$\delta_{\epsilon_1, \epsilon_2}(n) = 2|\mathcal{X}||\mathcal{Y}| \exp\left(-n \cdot \frac{(\epsilon_2 - \epsilon_1)^2}{1 + \epsilon_1} \cdot \mu_{XY} \right),$$

we state the following theorems.

Theorem G.2. *(Theorem 1.2 from [22]) Suppose* $0 \leq \epsilon_1 < \epsilon_2 \leq \mu_{XY}$*,* $(x^n, y^n) \in T^n_{\epsilon_1}(P_{XY})$*, and* (X^n, Y^n) *was emitted by the DMS* $P_{XY}(\cdot)$*. We have*

$$2^{-nH(Y|X)(1+\epsilon_1)} \leq P^n_{Y|X}(y^n|x^n) \leq 2^{-nH(Y|X)(1-\epsilon_1)} \tag{2.57}$$

$$(1-\delta_\epsilon(n))\, 2^{nH(Y|X)(1-\epsilon_2)} \leq \left|T^n_{\epsilon_2}(P_{XY}|x^n)\right| \leq 2^{nH(Y|X)(1+\epsilon_2)} \tag{2.58}$$

$$1-\delta_{\epsilon_1,\epsilon_2}(n) \leq Pr[Y^n \in T^n_{\epsilon_2}(P_{XY}|x^n)|X^n = x^n] \leq 1. \tag{2.59}$$

Theorem G.3. *(Theorem 1.3 from [22]) Consider a joint distribution* $P_{XY}(\cdot)$ *and suppose* $0 \leq \epsilon_1 < \epsilon_2 \leq \mu_{XY}$*,* Y^n *is emitted by a DMS* $P_Y(\cdot)$*, and* $x^n \in T^n_{\epsilon_1}(P_X)$*. We have*

$$(1-\delta_{\epsilon_1,\epsilon_2}(n))2^{-n[I(X;Y)+2\epsilon_2 H(Y)]} \leq \Pr[Y^n \in T^n_{\epsilon_2}(P_{XY}|x^n)] \leq 2^{-n[I(X;Y)-2\epsilon_2 H(Y)]}.$$

We next restate the Markov Lemma [23], which can be obtained as an application of *Theorem G.2.*

Lemma G.1. *(Markov Lemma) Let* $X - Y - Z$ *form a Markov chain. Also let* μ_{XYZ} *be the smallest positive value of* $P_{XYZ}(\cdot)$ *and* $0 \leq \epsilon_1 < \epsilon_2 \leq \mu_{XYZ}$*. Suppose that* $(x^n, y^n) \in T_{\epsilon_1}(P_{XY})$ *and* (X^n, Y^n, Z^n) *was emitted by the DMS* $P_{XYZ}(\cdot)$*, then* $\Pr[Z^n \in T^n_{\epsilon_2}(P_{XYZ}|x^n, y^n)|Y^n = y^n] \geq 1 - \delta_{\epsilon_1,\epsilon_2}(n)$*, where*

$$\delta_{\epsilon_1,\epsilon_2}(n) = 2|\mathcal{X}||\mathcal{Y}||\mathcal{Z}| \exp\left(-n \cdot \frac{(\epsilon_2-\epsilon_1)^2}{1+\epsilon_1} \cdot \mu_{XYZ}\right).$$

Next, we describe and analyze the HDA Costa scheme using the above results. The source is i.i.d with a probability distribution $P_V(\cdot)$ defined over a finite alphabet $\mathcal{V}$. The channel has an interference in the form of a sequence s^n that is an output of a DMS $P_S(\cdot)$. The channel is a discrete memoryless channel (DMC) characterized by the probability distribution $P_{Y|X,S}(\cdot)$, where x^n is the input to the channel and y^n is the output. At the receiver we form a reconstruction $\hat{v}^n$ from the received y^n. The channel input X, channel output Y, the interference S and the reconstruction $\hat{V}$ take values from the finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{S}$ and $\hat{\mathcal{V}}$, respectively. The distortion in reconstruction of the source is captured using a distortion function $d(\cdot)$, that maps $\mathcal{V} \times \hat{\mathcal{V}}$ to $\mathbb{R}^+$. The distortion for a sequence is expressed as

$$\overrightarrow{d}(v^n, \hat{v}^n) = \frac{1}{n} \sum_{i=1}^{n} d(v_i, \hat{v}_i).$$

Also we assume that there is a cost constraint for the channel input. The cost constraint is captured by a function $\rho(\cdot)$ that maps the input symbol $\mathcal{X}$ to $\mathbb{R}^+$. Also the average cost of transmission for a sequence is expressed as

$$\overrightarrow{\rho}(x^n) = \frac{1}{n} \sum_{i=1}^{n} \rho(x_i).$$

We also assume that both the channel input cost function $\rho(\cdot)$ and the distortion metric $d(\cdot)$ are bounded functions.

a. Code construction

We first form an auxiliary random variable U with alphabet $\mathcal{U}$. We consider U as an output of a channel $P_{U|S,V}(\cdot)$. We generate 2^{nR_a} codewords $u^n(w)$, $w = 1, 2, \ldots, 2^{nR_a}$, by choosing each of the $n \cdot 2^{nR_a}$ symbols $u_i(w)$ independently and at random according to $P_U(\cdot)$. The code book is revealed to both the encoder and the decoder.

b. Encoder

The encoder has a function $g(\cdot)$ that maps symbols in $\mathcal{U} \times \mathcal{S} \times \mathcal{V}$ to $\mathcal{X}$. The function $g(\cdot)$ acts component wise on the sequence (u^n, s^n, v^n) and the sequence mapping is expressed as $x^n = g^n(u^n, s^n, v^n)$, or in other words the sequence x^n will have $x_i = g(u_i, s_i, v_i)$ for all i. Given an observed interference s^n and source v^n, the encoder first attempts to find a w such that $(u^n(w), s^n, v^n) \in T_\epsilon^n(P_{USV})$. If the encoder finds an appropriate codeword $u^n(w)$, it transmits $x^n = g(u^n(w), s^n, v^n)$ through the channel. If the encoder fails to find such a w, then it transmits $x^n = g(u^n(1), s^n, v^n)$.

c. Decoder

The receiver observes y^n transmitted over the channel. Given y^n, the decoder attempts to find a $\tilde{w}$ such that $(u^n(\tilde{w}), y^n) \in T_\epsilon^n(P_{UY})$. If there are more than one $\tilde{w}$, the decoder randomly chooses a $\tilde{w}$ and if there is no such $\tilde{w}$, the decoder chooses $\tilde{w} = 1$. The decoder also has an estimation function ϕ that maps the symbols from $\mathcal{U} \times \mathcal{Y}$ to $\hat{\mathcal{V}}$. The decoder forms the sequence $\hat{v}^n$ as $\hat{v}_i = \phi(u_i, y_i)$ for all i. We also denote this operation as $\hat{v}^n = \phi^n(u^n, y^n)$. The decoder puts out the sequence $\hat{v}^n$ as its reconstruction of the source sequence.

d. Analysis of average distortion

We are interested in analyzing the average distortion achievable by the HDA scheme. The average distortion is expressed as

$$D = E[\overrightarrow{d}(V^n, \hat{V}^n)].$$

Here the expectation is taken over all the codebooks also. After obtaining a bound on D, we will finally show that at least one good code exists that achieves a distortion D.

We evaluate D by using *the law of total expectation* as follows,

$$E[\overrightarrow{d}(V^n, \hat{V}^n)] = \sum_{i=1}^{5} \Pr[\mathcal{E}_i] E\left[\overrightarrow{d}(V^n, \hat{V}^n) | \mathcal{E}_i\right], \tag{2.60}$$

where each of the events $\mathcal{E}_i$ are itemized and their probabilities bounded in the discussion that follows. Let us first have $0 < \epsilon_1 < \epsilon_2 < \epsilon_3 < \epsilon \leq \mu_{USVXY}$, where μ_{USVXY} is the smallest positive value of $P_{USVXY}(\cdot)$.

- $\mathcal{E}_1$: Suppose the observed $(s^n, v^n) \notin T^n_{\epsilon_1}(P_{SV})$. This is captured by the event $\mathcal{E}_1$. It can be shown from *Theorem G.1* that $\Pr[(S^n, V^n) \notin T^n_{\epsilon_1}(P_{SV})]$ is bounded above by $\delta_{\epsilon_1}(n)$, a function that approaches 0 with increasing n. If this event happens we can bound the average distortion by d_{max}, the maximum distortion of $d(\cdot)$, as $d(\cdot)$ was assumed to be bounded. Hence the first term in (2.60) can be bounded as,

$$\Pr[\mathcal{E}_1] E\left[\overrightarrow{d}(V^n, \hat{V}^n)|\mathcal{E}_1\right] \leq \delta_{\epsilon_1}(n) \cdot d_{max}$$

  and $\delta_{\epsilon_1}(n) \cdot d_{max}$ approaches 0 with increasing n.

- $\mathcal{E}_2$: Suppose the observed $(s^n, v^n) \in T^n_{\epsilon_1}(P_{SV})$, but the encoder can not find a w such that $(u^n(w), s^n, v^n) \in T^n_{\epsilon_2}(P_{USV})$. This event is captured by $\mathcal{E}_2$. We evaluate the probability of this event as follows

$$\begin{aligned}
\Pr[\mathcal{E}_2] &= \Pr\left[\bigcap_{w=1}^{2^{nR_a}} \left\{U^n(w) \notin T^n_{\epsilon_2}(P_{USV}|s^n, v^n)\right\}\right] \\
&\stackrel{(a)}{=} \left[1 - \Pr\left[U^n \in T^n_{\epsilon_2}(P_{USV}|s^n, v^n)\right]\right]^{2^{nR_a}} \\
&\stackrel{(b)}{\leq} \left[1 - (1 - \delta_{\epsilon_1,\epsilon_2}(n) 2^{-n[I(U;S,V)+2\epsilon_2 H(U)]}\right]^{2^{nR_a}} \\
&\stackrel{(c)}{\leq} \exp\left(-(1 - \delta_{\epsilon_1,\epsilon_2}(n)) 2^{n[R_a - I(U;S,V) - 2\epsilon_2 H(U)]}\right) \\
&\stackrel{(d)}{=} \delta_{\epsilon_1,\epsilon_2}(n, R_a)
\end{aligned} \tag{2.61}$$

  Here (a) follows because each of the codewords are chosen independently of each other and are from the same distribution $P_U(\cdot)$. (b) follows from the application of *Theorem G.2*. We obtain (c) by using the inequality $(1-x)^m \leq e^{-mx}$ and in

(d), we denote the bound on the probability of the event by $\delta_{\epsilon_1,\epsilon_2}(n, R_a)$. (2.61) suggests that we can choose large n and

$$R_a > I(U; S, V) + 2\epsilon_2 H(U), \tag{2.62}$$

to drive $\Pr[\mathcal{E}_2]$ to 0.

- Claim: *If* $(u^n(w), s^n, v^n) \in T^n_{\epsilon_2}(P_{USV})$*, then* $(u^n(w), s^n, v^n, x^n) \in T^n_{\epsilon_2}(P_{USVX})$ *and also we can establish that* $\overrightarrow{\rho}(x^n) \leq E[\rho(X)] + \epsilon_2 \cdot c_{max}$*, where* c_{max} *is the maximum value of the cost function* $\rho(\cdot)$*.*

  We can easily establish the above claim as follows. Notice that x^n is a deterministic function of (u^n, s^n, v^n) and is expressed as $x^n = g^n(u^n, s^n, v^n)$. Consider $\frac{1}{n}N(a, b, c, d|u^n, s^n, v^n, x^n)$. This can be expressed as,

$$\begin{aligned} \frac{1}{n}N(a, b, c, d|u^n, s^n, v^n, x^n) &= \begin{cases} \frac{1}{n}N(a, b, c|u^n, s^n, v^n) & \text{if } g(a, b, c) = d \\ 0, & \text{if } g(a, b, c) \neq d \end{cases} \\ &\stackrel{(a)}{\leq} \left(P_{USV}(a, b, c) + \epsilon_2 P_{USV}(a, b, c)\right) P_{X|USV}(d|a, b, c) \\ &= P_{USVX}(a, b, c, d) + \epsilon_2 P_{USVX}(a, b, c, d). \end{aligned} \tag{2.63}$$

  Here (a) follows by applying both the definition of the typical set $T^n_{\epsilon_2}(P_{USV})$, and also from the requirement that $d = g(a, b, c)$. By using similar arguments we can establish that if $(u^n(w), s^n, v^n) \in T^n_{\epsilon_2}(P_{USV})$, then $(u^n(w), s^n, v^n, x^n) \in T^n_{\epsilon_2}(P_{USVX})$.

  We will next establish the claim on the cost constraint. If $(u^n, s^n, v^n, x^n) \in T^n_{\epsilon_2}(P_{USVX})$, then it can be easily seen that $x^n \in T^n_{\epsilon_2}(P_X)$. Hence the cost can be evaluated as,

$$
\begin{aligned}
\overrightarrow{\rho}(x^n) &= \frac{1}{n}\sum_{i=1}^{n}\rho(x_i) \\
&\overset{(a)}{=} \sum_{a\in \text{supp}(P_X)} \frac{1}{n}N(a|x^n)\rho(a) \\
&\overset{(b)}{\leq} \sum_{a\in \text{supp}(P_X)} P_X(a)\rho(a) + \epsilon_2 \sum_{a\in \text{supp}(P_X)} P_X(a)\rho(a) \\
&\overset{(c)}{\leq} E[\rho(X)] + \epsilon_2 \cdot c_{max}
\end{aligned}
$$

Here (a) and (b) follow from the definition of the typical set $T^n_{\epsilon_2}(P_X)$. (c) follows as we bound the cost function with its maximum cost c_{max}.

- $\mathcal{E}_3$: Suppose $(u^n(w), s^n, v^n, x^n) \in T^n_{\epsilon_2}(P_{USVX})$, but $(u^n(w), y^n) \notin T^n_{\epsilon_3}(P_{UY})$, where y_i is chosen such that $P_{Y|SX}(\cdot|s_i, x_i(u_i, s_i, v_i))$ for all i, and $Y - [S, X] - [U, V]$. Since we have the Markov chain $U - [S, X] - Y$, Lemma G.1 (Markov Lemma) can be applied to show that the probability of this event (which we will denote by $\delta_{\epsilon_3}(n)$) is small for large n.

- $\mathcal{E}_4$: Suppose $(u^n(w), y^n) \in T^n_{\epsilon_3}(P_{UY})$, but the decoder finds a $\tilde{w} \neq w$ such that $(u^n(\tilde{w}), y^n) \in T^n_{\epsilon}(P_{UY})$. This event is captured by $\mathcal{E}_4$. Since, each of the codewords are drawn i.i.d according to a distribution $P_U(\cdot)$, the probability that a randomly chosen $u^n(\tilde{w})$ is jointly typical with the observed y^n can be captured using *Theorem G.3*. Hence

$$
\begin{aligned}
\Pr[\mathcal{E}_4] &= \Pr\left[\bigcup_{\tilde{w}\neq w}((U^n(\tilde{w}), y^n) \in T_\epsilon^n(P_{UY}))\right] \\
&\overset{(a)}{\leq} \sum_{\tilde{w}\neq w} \Pr\left[((U^n(\tilde{w}), y^n) \in T_\epsilon^n(P_{UY}))\right] \\
&\overset{(b)}{=} (2^{nR_a} - 1)\Pr\left[((U^n, y^n) \in T_\epsilon^n(P_{UY}))\right] \\
&\overset{(c)}{\leq} (2^{nR_a} - 1)2^{-n(I(U;Y)-2\epsilon H(U))} \\
&\overset{(d)}{=} \delta_\epsilon(n, R_a)
\end{aligned}
$$

Here (a) follows from the union bound and (b) follows from the symmetry of codeword generation. We obtain (c) by applying *Theorem G.3* and in (d), we denote the bound on the probability of the event by $\delta_\epsilon(n, R_a)$.

- $\mathcal{E}_5$: Finally $\mathcal{E}_5$ is the event that the encoder found a typical $u^n(w)$ and the decoder was able to decode to the chosen w. The distortion in the reconstruction when this event happens can be evaluated as follows. Since, $(u^n(w), v^n, y^n) \in T_\epsilon^n(P_{UVY})$, we have

$$
\begin{aligned}
\overrightarrow{d}(v^n, \hat{v}^n) &= \overrightarrow{d}(v^n, \phi^n(u^n(w), y^n)) \\
&= \frac{1}{n}\sum_{i=1}^{n} d(v_i, \phi(u_i(w), y_i)) \\
&= \frac{1}{n}\sum_{a,b,c} N(a,b,c|u^n(w), v^n, y^n) d(b, \phi(a,c)) \\
&\leq \sum_{a,b,c} P_{UVY}(a,b,c)(1+\epsilon) d(b, \phi(a,c)) \\
&\leq E[d(V, \phi(U,Y))] + \epsilon \cdot d_{max} \qquad (2.64)
\end{aligned}
$$

Hence we can evaluate (2.60) by combining all the above results as shown below.

$$\begin{aligned}
E[\overrightarrow{d}(V^n,\hat{V}^n)] &= \sum_{i=1}^{5}\Pr[\mathcal{E}_i]E\left[\overrightarrow{d}(V^n,\hat{V}^n)|\mathcal{E}_i\right] \\
&= \sum_{i=1}^{4}\Pr[\mathcal{E}_i]E\left[\overrightarrow{d}(V^n,\hat{V}^n)|\mathcal{E}_i\right] + \Pr[\mathcal{E}_5]E\left[\overrightarrow{d}(V^n,\hat{V}^n)|\mathcal{E}_5\right] \\
&\le (\delta_{\epsilon_1}(n) + \delta_{\epsilon_1,\epsilon_2}(n,R_a) + \delta_{\epsilon_3}(n) + \delta_{\epsilon}(n,R_a)) \cdot d_{max} \\
&\quad + 1 \cdot (E[d(V,\phi(U,Y))] + \epsilon \cdot d_{max}) \qquad (2.65)
\end{aligned}$$

Hence by choosing R_a such that

$$I(U;S,V) < R_a < I(U;Y),$$

we can find an ϵ_2 and an ϵ small enough such that,

$$I(U;S,V) + 2\epsilon_2 H(U) < R_a < I(U;Y) - 2\epsilon H(U).$$

Now by choosing n large enough, the average distortion can be bounded by $E[d(V,\phi(U,Y))]+2\epsilon \cdot d_{max}$ and the average channel input cost can be bounded by $E[\rho(X)] + 2\epsilon_2 \cdot c_{max}$. In other words, for $n \to \infty$ an average distortion of $E[d(V,\phi(U,Y))]$ can be achieved under the cost constraint of $E[\rho(X)]$. Since the average distortion over the ensemble of codebooks is bounded by $E[d(V,\phi(U,Y))]$ under the average cost constraint of $E[\rho(X)]$, it can be easily seen that there exists at least one good code satisfying the average cost constraint, and also achieves the required distortion. We summarize this result as a lemma which is given below.

Lemma G.2. *For a given channel encoding function $g(\cdot)$, joint probability distribution $P_{USVXY}(\cdot)$ with the Markov chain $[U,V]-[S,X]-Y$, channel distribution $P_{Y|XS}(\cdot|x_i,s_i)$, an average input cost constraint $E[\rho(X)]$, source estimator $\phi(\cdot)$, if $I(U;Y) > I(U;S,V)$, there exists an HDA Costa code such that the average distor-*

tion in estimating the source V can be bounded by $E[d(V, \phi(Y, U))] + \epsilon$, where $\epsilon \to 0$ as $n \to \infty$.

e. Some comments

Though the above results are for the finite alphabet case, they can be extended to the real continuous sources and distortion metrics by following similar steps as in [12]. Hence we can obtain results for the Gaussian case too. We can also repeat these arguments for the HDA Wyner-Ziv and the other HDA schemes considered in this work. Similarly the results could be extended for a degraded channel case also. Assume that there are L receivers that receive $Y_i, i \in 1, 2, \ldots L$ and assuming we have the Markov chain $Y_1 - Y_2 - Y_3 - \ldots - Y_L$, we can repeat the same proof to show that over the ensemble of codebooks, the average distortion can be bounded by $E[d(V, \phi_i(U, Y_i))]$ for every receiver $i \in 1, 2, \ldots L$. Hence, it can be seen that there is at least one code that can simultaneously achieve these distortions. Hence, by using continuity arguments for the Gaussian channel case, with a given minimum and maximum possible channel SNR, we can always design a code that obtains the claimed distortion over the given SNR range. This result is used in section E in the analysis of HDA coding for SNR mismatch.

CHAPTER III

APPLICATIONS OF JSCC

In this chapter we study several applications of the schemes introduced in the previous chapter. A natural scenario where the interference in the channel is known at the transmitter, is a case where the interference is introduced by the transmitter itself. This can happen in the case of transmitting an analog source with bandwidth compression say when two symbols of the source have to be transmitted in one channel use. In this case one symbol acts as the interference to the other and this interference is known at the transmitter. HDA Costa schemes can be applied for this setup and this is one of the applications discussed in this work.

Another application discussed is the cognitive radio setup. In this case there is a primary transmitter that transmits information to it's intended receiver. There is also a secondary communication system, that has access to the primary transmitter information. The goal of the secondary communication system is to transmit some information to it's users without degrading the performance of the primary system. The secondary user hence sees an interference(primary transmitter signal) in the channel that is known already at the transmitter.

The final application that we consider is the case of JSCC under a physical layer security requirement. We consider the transmission of a analog Gaussian source to an intended receiver in the presence of an eavesdropper. The goal is to provide a graceful degradation of distortion with SNR for the intended receiver, while keeping the eavesdropper's information content of the analog source to the minimum. We next present below the main results presented in this chapter.

A. Main results

- We propose JSCC schemes for broadcasting an analog source with bandwidth compression. Specifically we study the distortion region for broadcasting an analog source to two users with different receiver channel SNRs. We show that the two user distortion region obtained by our proposed HDA scheme performs close to the best known schemes for this setup. This is discussed in sections B and C.

- We propose a JSCC scheme for communicating an analog Gaussian source in the presence of an eavesdropper. The scheme proposed provides a graceful degradation in distortion with SNR for the intended receiver, for a small fixed information leakage to the eavesdropper. This is studied in section D.

- We also propose JSCC schemes for the cognitive setup, where the cognitive users have complete knowledge of the primary transmitter's output signal. We show that it is possible to obtain a graceful degradation for the cognitive users, while maintaining the original performance of the primary system. This is discussed in section E.

B. Applications to transmitting a Gaussian source with bandwidth compression

We now consider the problem of transmitting K samples of the i.i.d Gaussian source to a single user in $N = \lambda K$ ($\lambda < 1$, $1/\lambda$ is an integer) uses of an AWGN channel with noise variance σ^2 where the transmit power is constrained to be 1. There is no interference in the channel, but since $\lambda < 1$, we will see that the techniques described in the previous chapter are useful for this problem.

There are at least three ways to achieve the optimal distortion in this case.

One is to use a conventional separation based approach. The second one is to use superposition coding and the third one is to use Costa coding. Although, they are all optimal for the single user case, they perform differently when there is a mismatch in the channel SNR and, hence, the last two approaches are briefly described here. Other schemes to achieve the optimal distortion can also be found in [5], [24] and [10].

Superposition coding: Here we split the source in two parts and take N samples of the source $\mathbf{v}$, namely v_1^N and scale it by $\sqrt{a}$ creating the systematic signal $\mathbf{x}_1 = \sqrt{a}v_1^N$. We take the other $K-N$ source samples v_{N+1}^K and use a conventional source encoder followed by a capacity achieving channel code resulting in the N dimensional vector $\mathbf{x}_c = \mathcal{C}(\mathcal{Q}(v_{N+1}^K))$, where $\mathcal{C}$ denotes a channel encoding operation and $\mathcal{Q}$ denotes a source encoding operation. Then $\mathbf{x}_c$ is normalized so that the average power is $\sqrt{1-a}$. The overall transmitted signal is $\mathbf{x} = \mathbf{x}_s + \mathbf{x}_c$ and the received signal is $\mathbf{y} = \mathbf{x} + \mathbf{w}$. At the receiver, the digital part is first decoded assuming the systematic (analog) part is noise and then $\mathbf{x}_c$ is subtracted from $\mathbf{y}$. Then an MMSE estimate of v_1^N given by $\hat{\mathbf{v}}_1^N = \frac{\sqrt{a}}{a+\sigma^2}(\mathbf{y} - \mathbf{x}_c)$ is formed. The distortion as a function of a is given by

$$D(a) = \frac{\lambda}{1+\frac{a}{\sigma^2}} + \frac{1-\lambda}{(1+\frac{1-a}{a+\sigma^2})^{\lambda/(1-\lambda)}}.$$

For the optimal choice of a, the overall distortion is given by

$$a^*_{sup} = \sigma^2\left[\left(1+\frac{1}{\sigma^2}\right)^{\lambda} - 1\right] \text{ and } D^*_{sup} = \frac{1}{\left(1+\frac{1}{\sigma^2}\right)^{\lambda}} \tag{3.1}$$

which is the optimal distortion.

Digital Costa coding: We split the source exactly as in the previous case and one stream is formed as $\mathbf{x}_s = \sqrt{a}v_1^N$. However, here the digital part assumes that $\mathbf{x}_s$

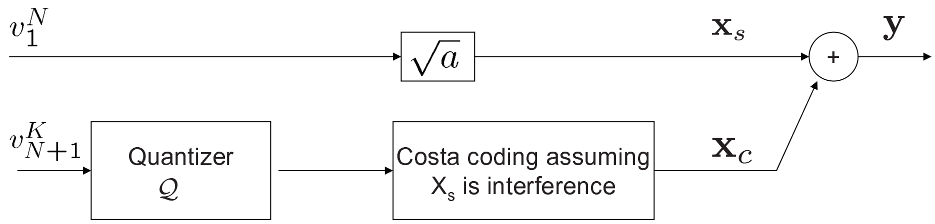

Fig. 8. Encoder model using Costa coding for single user.

is interference and uses Costa coding to produce $\mathbf{x}_c$ with power $1-a$ as shown in Fig. 8. In Costa coding, we define an auxiliary random variable $\mathbf{u} = \mathbf{x}_c + \alpha_1 \mathbf{x}_s$ where $\alpha_1 = \frac{1-a}{1-a+\sigma^2}$ is the optimum scaling coefficient. At the receiver, the digital part is decoded which means that $\mathbf{u}$ can be obtained. In spite of knowing $\mathbf{u}$ exactly, the optimal estimate of v_1^N is obtained by simply treating $\mathbf{x}_c$ as noise since for the optimal choice of α_1, $\mathbf{x}_c = \mathbf{u} - \alpha_1 \mathbf{x}_s$ and v_1^N are uncorrelated. Therefore, an MMSE estimate of v_1^N is formed assuming $\mathbf{x}_c$ were noise. Hence, the overall distortion becomes

$$D = \frac{\lambda}{1 + \frac{a}{1-a+\sigma^2}} + \frac{1-\lambda}{\left(1 + \frac{1-a}{\sigma^2}\right)^{\lambda/1-\lambda}} \tag{3.2}$$

Again, minimizing D w.r.t. a gives

$$a^*_{costa} = (1+\sigma^2)\left[1 - \frac{1}{\left(1+\frac{1}{\sigma^2}\right)^{\lambda}}\right] \text{ and } D^*_{costa} = \frac{1}{\left(1+\frac{1}{\sigma^2}\right)^{\lambda}} \tag{3.3}$$

which is the best possible distortion.

Hybrid digital analog Costa coding: For the case of $\lambda = 0.5$, the digital Costa coding part can be replaced with a hybrid digital analog (HDA) Costa coding. We refer to such a scheme as HDA Costa coding. The power allocation to the layers remains the same as in the digital Costa coding scheme and, hence, we can simply use a^*_{Costa} without the need to differentiate the digital and HDA Costa coding. It is quite straightforward to show that $a^*_{Costa} > a^*_{sup}$ for $\lambda < 1$. Hence, the Costa coding approach allocates higher power to the systematic part than the superposition approach, since the systematic part is treated as interference.

1. Performance in the presence of SNR mismatch

Now, we consider the same set up as above, but when the actual channel noise variance is σ_a^2, whereas the designed noise variance is σ^2.

Case 1: $\sigma_a^2 > \sigma^2$

The distortion for the superposition code can be computed to be the sum of the distortions in the systematic part and the digital part. When $\sigma_a^2 > \sigma^2$, the digital part cannot be decoded and, hence, we assume that the distortion in the digital part is the variance of the source, 1.

$$D_{sup} = \frac{\lambda}{1 + \frac{a^*_{sup}}{1 - a^*_{sup} + \sigma_a^2}} + (1 - \lambda) \cdot 1 \tag{3.4}$$

Both the digital and HDA Costa coding schemes perform identically when $\sigma_a^2 > \sigma^2$ and the distortion for the Costa code can be computed to be

$$D_{digCosta} = D_{HDACosta} = \frac{\lambda}{1 + \frac{a^*_{Costa}}{1 - a^*_{Costa} + \sigma_a^2}} + (1 - \lambda) \cdot 1 \tag{3.5}$$

Case 2: $\sigma_a^2 < \sigma^2$

In this case, the digital part can be decoded exactly and, hence, the distortion for superposition coding is

$$D_{sup} = \lambda \frac{1}{1 + \frac{a^*_{sup}}{\sigma_a^2}} + (1 - \lambda) \frac{1}{\left(1 + \frac{1 - a^*_{sup}}{a^*_{sup} + \sigma^2}\right)^{\lambda/(1-\lambda)}}. \tag{3.6}$$

For digital Costa coding, the decoder first decodes the digital part when the auxiliary random variable $\mathbf{u}$ is perfectly known. In the case when $\sigma_a^2 \neq \sigma^2$, the receiver must form the MMSE estimate of v_1^N from the channel observation $\mathbf{y}$ and $\mathbf{u}$. Therefore, the overall distortion is

$$\begin{aligned} D_{digCosta} =& \lambda \Bigg(1 - [\sqrt{a^*_{Costa}}\ \alpha\sqrt{a^*_{Costa}}] \\ & \times \begin{bmatrix} 1+\sigma_a^2 & 1-a^*_{Costa}+\alpha a^*_{Costa} \\ 1-a^*_{Costa}+\alpha a^*_{Costa} & 1-a^*_{Costa}+\alpha^2 a^*_{Costa} \end{bmatrix}^{-1} \\ & \times \begin{bmatrix} \sqrt{a^*_{Costa}} \\ \alpha\sqrt{a^*_{Costa}} \end{bmatrix}\Bigg) + (1-\lambda)\frac{1}{\left(1+\frac{1-a^*_{Costa}}{a^*_{Costa}+\sigma^2}\right)^{\lambda/(1-\lambda)}}. \end{aligned}$$

For the HDA Costa coding, we can decode $\mathbf{u}$ and form MMSE estimates of v_1^N and v_{N+1}^K separately and, hence, the overall distortion is given by

$$\begin{aligned} D_{HDACosta} =& \lambda \Bigg(1 - [\sqrt{a^*_{Costa}}\ \alpha\sqrt{a^*_{Costa}}] \\ & \times \begin{bmatrix} 1+\sigma_a^2 & 1-a^*_{Costa}+\alpha a^*_{Costa} \\ 1-a^*_{Costa}+\alpha a^*_{Costa} & 1-a^*_{Costa}+\alpha^2 a^*_{Costa}+\kappa^2 \end{bmatrix}^{-1} \\ & \times \begin{bmatrix} \sqrt{a^*_{Costa}} \\ \alpha\sqrt{a^*_{Costa}} \end{bmatrix}\Bigg) + (1-\lambda)\,(1-[0\ \kappa] \\ & \times \begin{bmatrix} 1+\sigma_a^2 & 1-a^*_{Costa}+\alpha a^*_{Costa} \\ 1-a^*_{Costa}+\alpha a^*_{Costa} & 1-a^*_{Costa}+\alpha^2 a^*_{Costa}+\kappa^2 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ \kappa \end{bmatrix}\Bigg). \end{aligned}$$

The performance of the superposition scheme, digital Costa and HDA Costa scheme are shown for an example with $\lambda = 0.5$ in Fig. 9. The designed SNR is defined as $10\log_{10}\frac{1}{\sigma^2}$ whereas the actual SNR is defined as $10\log_{10}\frac{1}{\sigma_a^2}$. In the example, the designed SNR is fixed at 10dB and the actual SNR is varied from 0 dB to 20 dB. It can be seen that the Costa coding approach is better than superposition coding when

$\sigma_a^2 > \sigma^2$ and worse for the other case. The HDA Costa coding scheme performs the best over the entire range of SNRs.

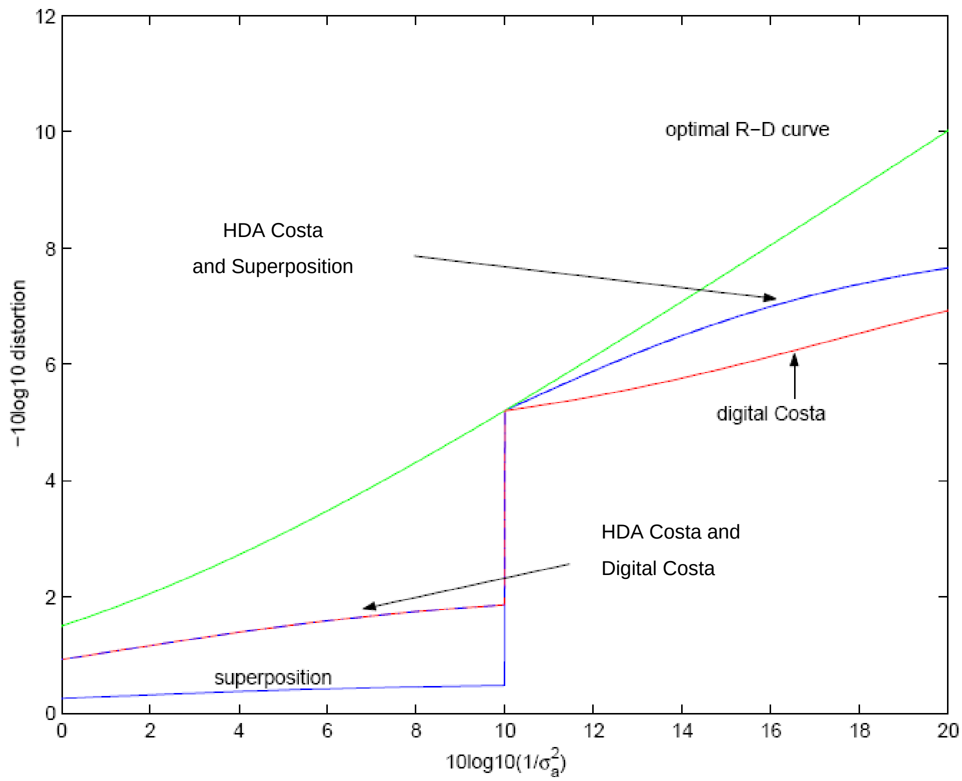

Fig. 9. Performance of different schemes for the source splitting approach for the bandwidth compression problem with SNR mismatch.

C. Applications to broadcasting with bandwidth compression

We now consider the problem of transmitting $K = 2N$ samples of a unit variance Gaussian source $\mathbf{v}$ in N uses of the channel to two users through AWGN channels with noise variances σ_1^2 (weak user) and σ_2^2 (strong user) with $\sigma_1 > \sigma_2$. The channel has the power constraint $P = 1$. We are interested in joint source channel coding schemes that provide a good region of pairs of distortion that are simultaneously achievable at the two users. This problem was considered in [5, 24, 25]. The best known region to date is given by the schemes therein.

Notice that when we design a source channel coding scheme to be optimal for the weak user, the strong user operates under the situation of SNR mismatch explained in chapter II-E.1 with $\sigma_2^2 = \sigma_a^2 < \sigma^2 = \sigma_1^2$. Similarly, when the system is designed to be optimal for the strong user, for the weak user $\sigma_1^2 = \sigma_a^2 > \sigma^2 = \sigma_2^2$. Motivated by the fact that for $\lambda = 0.5$, the HDA Costa coding scheme performs the best, we propose a scheme which is shown in Fig. 10.

There are three layers in the proposed coding scheme. The first layer is the systematic part where N out of the K samples of the source are scaled by $\sqrt{a}$. Let us call this as $\mathbf{x}_s = \sqrt{a}v_1^N$. The other $K - N$ samples of the Gaussian source are hybrid digital analog Costa coding, treating $\mathbf{x}_s$ as the interference and transmits the signal $\mathbf{x}_1$ with power b in the second layer. So $\mathbf{x}_1 = \mathbf{u}_1 - \alpha_1\mathbf{x}_s - \kappa_c v_{N+1}^K$, where α_1 and κ_c are the optimal scaling coefficient to be used in the hybrid digital analog Costa coding process and $\mathbf{u}_1$ is the auxiliary variable. This layer is meant to be decoded by the weak user and, hence, the scaling factor α_1 is set to be $b/(b+c+\sigma_1^2)$. That is, this layer sees the third layer also as *independent* noise. The third layer is first Wyner-Ziv coded at a rate R_2 assuming the estimate of v_{N+1}^K at the receiver as source side information. The Wyner-Ziv index is then encoded using digital Costa coding assuming $\mathbf{x}_s$ and $\mathbf{x}_1$ are interference and uses power $c = 1 - a - b$. Therefore, $\mathbf{x}_2 = \mathbf{u}_2 - \alpha_2(\mathbf{x}_s + \mathbf{x}_1)$. This layer is meant for the strong user and, hence, the scaling factor $\alpha_2 = c/(c + \sigma_2^2)$. We then transmit $\mathbf{x} = \mathbf{x}_s + \mathbf{x}_1 + \mathbf{x}_2$.

At the receiver, from the second layer an estimate of v_{N+1}^K is obtained. This estimate acts as source side information that can be used in refining the estimate of v_{N+1}^K for the strong user using the decoded Wyner-Ziv bits. The Wyner-Ziv bits are

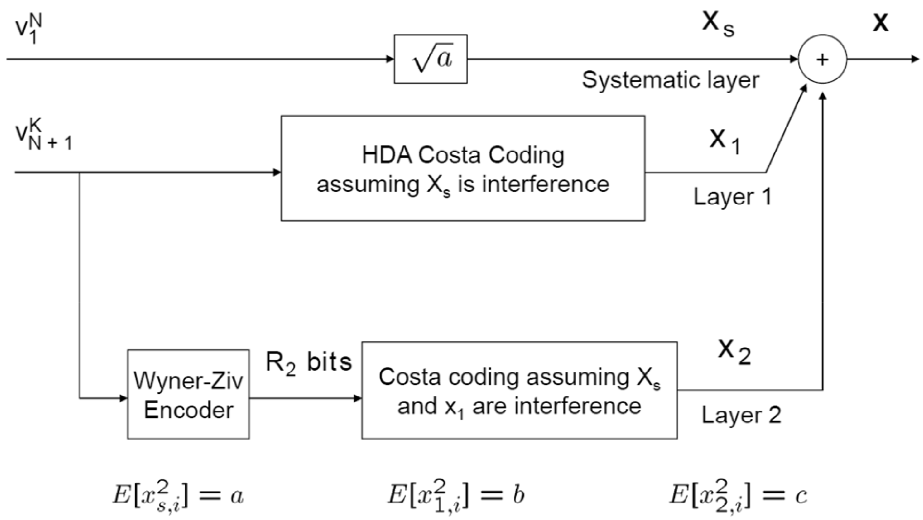

Fig. 10. Encoder model using Costa coding.

decoded from the third layer by Costa decoding procedure.

The users estimate the systematic part v_1^N and non-systematic part v_{N+1}^K by MMSE estimation from the received $\mathbf{y}$, the decoded $\mathbf{u}_1$ and $\mathbf{u}_2$. So the overall distortion seen at the weak user is

$$D_1 = \frac{1}{2}\frac{1}{1+\frac{a}{b+c+\sigma_1^2}} + \frac{1}{2}\frac{1}{1+\frac{b}{c+\sigma_1^2}}.$$

The distortion for the strong user is given by

$$\begin{aligned} D_2 =& \frac{1}{2}\left(1 - [\sqrt{a}\ \alpha_1\sqrt{a}]\begin{bmatrix} 1+\sigma_2^2 & b+\alpha_1 a \\ b+\alpha_1 a & b+\alpha_1^2 a+\kappa_c^2 \end{bmatrix}^{-1}\begin{bmatrix} \sqrt{a} \\ \alpha_1\sqrt{a} \end{bmatrix}\right) \\ &+ \frac{1/2}{1+\frac{c}{\sigma_2^2}}\left(1 - [0\ \kappa_c]\begin{bmatrix} 1+\sigma_2^2 & b+\alpha_1 a \\ b+\alpha_1 a & b+\alpha_1^2 a+\kappa_c^2 \end{bmatrix}^{-1}\begin{bmatrix} 0 \\ \kappa_c \end{bmatrix}\right). \end{aligned}$$

The corner points of the distortion region corresponding to being optimal for the strong and weak user respectively, can be obtained by setting $b = 0$ and $c = 0$, respectively.

The distortion region for this scheme for the case of $\sigma_1^2 = 0$ dB and $\sigma_2^2 = -5$ dB is shown in Fig. 11. The distortion region for three other schemes are also shown. They are the scheme proposed by Mittal and Phamdo in [5] , a different broadcasting scheme which uses digital Costa coding in both the layers proposed in [25] (details can be found there) and the broadcast scheme with one layer of superposition coding and one layer of digital Costa coding considered in [24, 25]. The scheme in [24, 25] currently appears to be the best known scheme. Notice that in the third layer, instead of using a separate Wyner-Ziv encoder followed by a Costa code, we could have used the HDA scheme discussed in Section D with identical results.

The proposed broadcast scheme in Fig. 10 significantly outperforms the scheme in Mittal and Phamdo and the digital Costa based broadcast scheme for this example. The corner points of this scheme also coincide with those of the best known schemes reported in [24, 25].

D. JSCC for secrecy systems

In this section, we consider the transmission of a Gaussian source over a Gaussian channel having an input power constraint, in the presence of an eavesdropper. We are interested in estimating the source at the intended receiver with the minimum possible distortion. For a fixed information leakage I_ϵ to the eavesdropper, we propose a scheme which achieves the minimal possible distortion for a given design SNR of snr, and also provides a graceful degradation of distortion with SNR.

The source $V \sim \mathcal{N}(0, \sigma_v^2)$ is an N-length discrete time real Gaussian source and

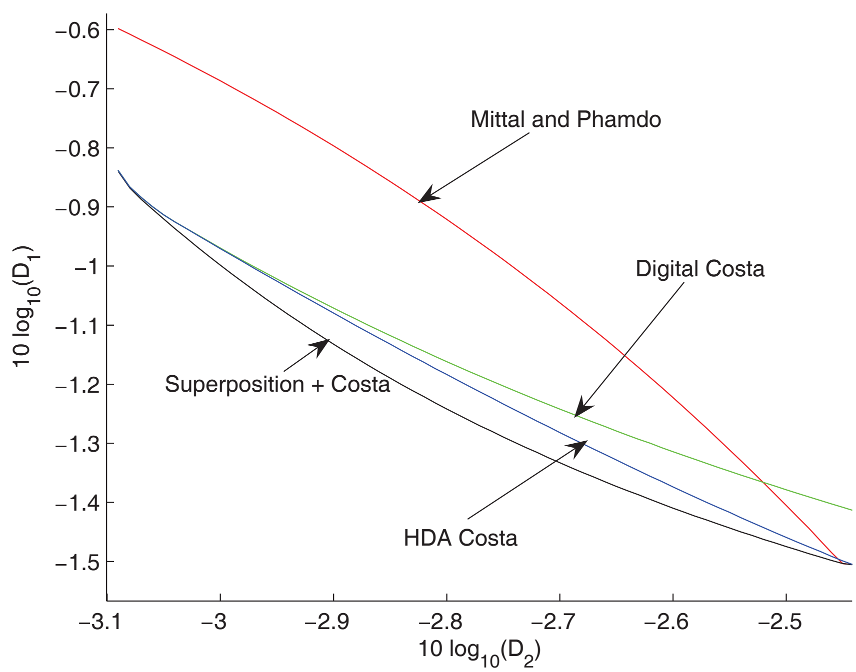

Fig. 11. Distortion regions of the different schemes for broadcasting with bandwidth compression.

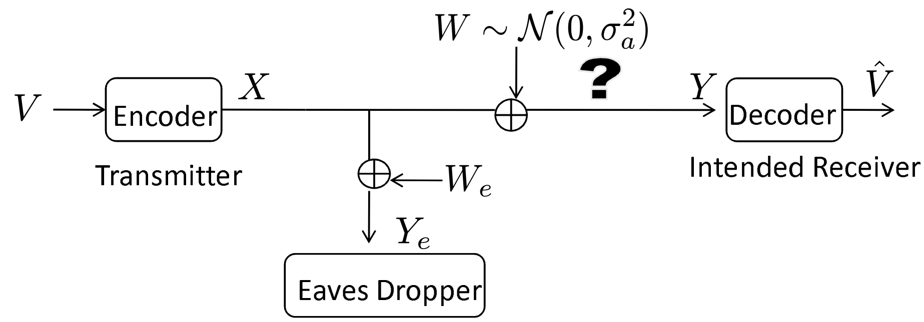

Fig. 12. Problem model for the Secrecy system.

the channel is a discrete time real Gaussian wiretap channel [26] as shown in Fig. 12. The source and channel bandwidths are assumed to be matched and hence the input to the channel is a n-length vector $\mathbf{x}$, which is also assumed to have an average power constraint of P expressed as $E[X^2] \leq P$. The received signal at the eavesdropper $\mathbf{y_e}$ can be expressed as

$$\mathbf{y_e} = \mathbf{x} + \mathbf{w_e}.$$

Here $\mathbf{w_e}$ is the N-length additive white Gaussian noise(AWGN) vector having zero mean and noise variance of σ_e^2. The intended receiver receives the N-dimensional vector $\mathbf{y}$ given by

$$\mathbf{y} = \mathbf{x} + \mathbf{w},$$

where the noise $\mathbf{w}$ is the N-length additive white Gaussian noise vector having zero mean and noise variance of σ_a^2. The transmitter does not have an exact knowledge of σ_a^2 but knows that $\sigma_a^2 \leq \sigma^2$, where σ^2 is the noise variance corresponding to some design SNR. The eavesdropper channel is a degraded version of the main channel and is assumed to have the lowest SNR i.e. $\mathsf{snr}_e < \mathsf{snr} < \mathsf{snr}_a$, where we define $\mathsf{snr}_e := P/\sigma_e^2$, $\mathsf{snr} := P/\sigma^2$ and $\mathsf{snr}_a := P/\sigma_a^2$. The receiver is assumed to have a perfect estimate of snr_a, but the transmitter is assumed to be kept ignorant of this information.

We refer to the information leaked to the eavesdropper as the information leakage rate and is expressed as $I_\epsilon := \frac{1}{N} I(\mathbf{V}; \mathbf{Y_e})$. The information leakage rate is the difference between the average source entropy $\frac{1}{N} h(\mathbf{V})$ and the equivocation rate $\frac{1}{N} h(\mathbf{V}|\mathbf{Y_e})$ defined in [26] and [27]. It is fairly common to use equivocation rate in literature, but since we have a continuous source, the equivocation rate expressed as differential entropy may not be always positive. Therefore, we choose the metric as the mutual information between the source and the received signal which is always ≥ 0. Notice that $I_\epsilon = 0$ corresponds to perfect secrecy, and this implies that the eavesdropper gains no information about the source.

The intended receiver makes an estimate $\hat{\mathbf{v}}$ of the analog source $\mathbf{v}$ from the observed vector $\mathbf{y}$. The distortion in estimating V can be expressed as $D(\mathsf{snr}_a) = E[(V - \hat{V})^2]$, where $\mathsf{snr}_a = P/\sigma_a^2$. In this work, for a fixed information leakage rate I_ϵ, we are interested in schemes which are optimal for snr and which also provide a low source distortion for $\mathsf{snr}_a > \mathsf{snr}$.

Before introducing our proposed schemes, we would like to mention some prior work in this area. There has been a considerable amount of work in studying the graceful degradation of distortion with SNR for both the bandwidth matched case [7] and the bandwidth mismatched case, and several joint source channel coding schemes have been proposed [5]. There also exists a considerable amount of literature on physical layer security. The wire-tap channel was first introduced and studied by Wyner in [26], and the Gaussian wire-tap channel was studied by Leung and Hellman in [27]. In [28], Yamamoto studied the Shannon cipher system from a rate distortion perspective, where in one of the theorems it is shown that for a wiretap channel with a fixed SNR, a separation based approach of quantization followed by secrecy coding is optimal. However in this work, in contrast to [28] we are interested in JSCC scheme for the Gaussian wiretap channel under the SNR mismatch case. We are also interested in quantifying the graceful degradation of distortion with SNR.

1. A separation based scheme and a simple scaling scheme

For the classical setup without the eavesdropper, both the uncoded scheme and the separation based scheme can be observed to be optimal for a given SNR. However these schemes perform differently in the presence of a SNR mismatch. In this section we look at the performance of both the separation based scheme and the uncoded scheme in the presence of an eavesdropper.

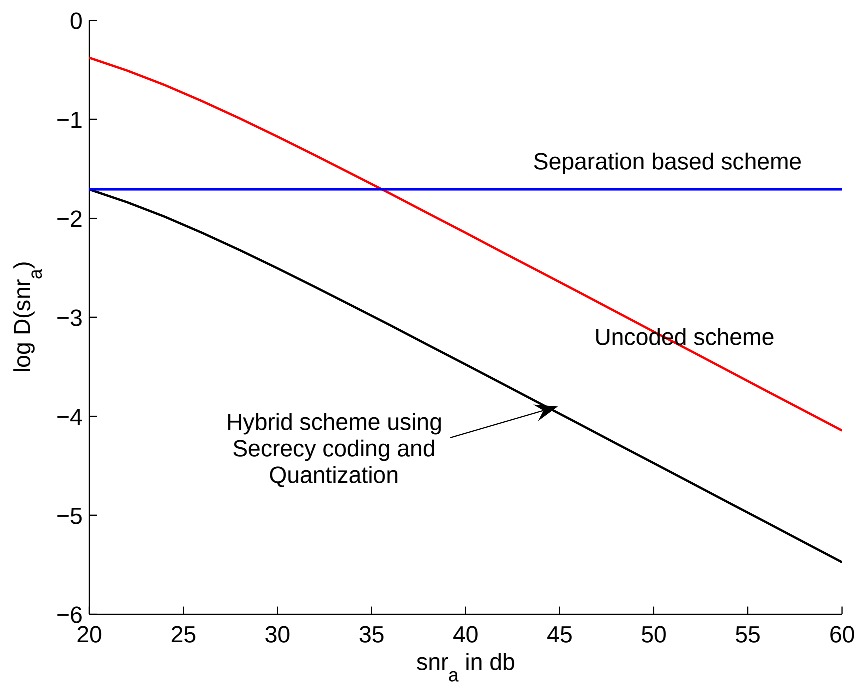

Fig. 13. Distortion vs snr_a for different schemes for $I_\epsilon = 0.01$. Here $P = 1$, $\sigma_e^2 = 1$ and $\sigma^2 = 0.01(\mathsf{snr} = 20db)$.

a. Separation based scheme

Here we use a separation based scheme designed for a channel noise variance of σ^2 and information leakage I_ϵ. We first design a vector quantizer of rate

$$R_v = C\left(\frac{P}{\sigma^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + I_\epsilon,$$

where $C(x) := \frac{1}{2}\log(1+x)$. We quantize $\mathbf{v}$ to $\mathbf{v}_q$ using the designed vector quantizer of rate R_v. $\mathbf{v}_q$ is then mapped to $\mathbf{v}_{sec}$ using a secrecy code as in [27]. The encoded $\mathbf{v}_{sec}$ is transmitted over the channel. The eavesdropper obtains a maximum leakage rate of I_ϵ. The proof of this claim is given at the end of this section. The intended receiver achieves a distortion of $\sigma_v^2 2^{-2R_v}$. Since we have quantized the source to a fixed rate, the achievable distortion is constant for all SNRs above the designed SNR and is given by,

$$D(\mathsf{snr}_a) = \sigma_v^2 2^{-2R_v} < \sigma_v^2.$$

For the given I_ϵ, though we get some improvement in distortion, the exponent is 0 and we do not have a graceful degradation of distortion with SNR as shown in Fig. 13.

b. A simple scaling scheme

Let us first consider a scheme that is optimal for all channel SNRs for the Gaussian wiretap channel in the absence of the eavesdropper. This reduces to the classical problem of point to point communication over a Gaussian channel. An optimal scheme is scaling the analog source $\mathbf{v}$ by a constant $\kappa = \sqrt{P/\sigma_v^2}$ to match the transmit power constraint [7]. The transmitted vector is hence given by $\mathbf{x} = \kappa\mathbf{v}$. The receiver has perfect knowledge of snr_a and obtains a minimum mean square estimate of $\mathbf{v}$ from the observed $\mathbf{y}$. The distortion obtained at the intended receiver is given by

$$D(SNR_a) = \frac{\sigma_v^2}{1 + \mathsf{snr}_a}.$$

The distortion exponent can be seen to be -1 for this scheme and also the obtained distortion is optimal for every given snr_a. The information leakage rate is easily calculated to be

$$\frac{1}{n} I(\mathbf{V}; \mathbf{Y_e}) = I(V; Y_e) = \frac{1}{2} \log \left(1 + \frac{\kappa^2 \sigma_v^2}{\sigma_e^2}\right) = \frac{1}{2} \log \left(1 + \frac{P}{\sigma_e^2}\right).$$

From the above equation we can observe that the choice of $\kappa = \sqrt{\frac{P}{\sigma_v^2}}$ results in a reasonably high information leakage rate. However, we can reduce the value of κ to satisfy our eavesdropper information requirement of I_ϵ as follows by choosing

$$I_\epsilon = \frac{1}{2} \log(1 + \frac{\kappa^2 \sigma_v^2}{\sigma_e^2})$$

or

$$\kappa^2 = \frac{\sigma_e^2}{\sigma_v^2}(2^{2I_\epsilon} - 1).$$

The intended receiver receives $\mathbf{y} = \kappa \mathbf{v} + \mathbf{w}$. Hence the distortion at the intended receiver is given by

$$D(\mathsf{snr}_a) = \frac{\sigma_v^2}{1 + \frac{\kappa^2 \sigma_v^2}{\sigma_a^2}} = \frac{\sigma_v^2}{1 + \frac{\kappa^2 \sigma_v^2 \mathsf{snr}_a}{P}}.$$

Hence for $\mathsf{snr}_a = \mathsf{snr}$, $D(\mathsf{snr}) > \sigma_v^2/(1 + \mathsf{snr})$ as $\kappa^2 \sigma_v^2 < P$. Though the above equation shows that the distortion exponent is -1, we have a considerable loss in optimality at the intended receiver, as we have not used the full power P at the transmitter. This can be seen from Fig. 13 where for $\mathsf{snr}_a = 20$db, we see that the uncoded scheme has a higher distortion performance compared to the separation based scheme. However we can see from Fig. 13 that the uncoded scheme gives a graceful degradation in distortion, unlike the separation based scheme. Also if we need $I_\epsilon = 0$, then κ must be chosen to be 0 and hence $D(\mathsf{snr}) = \sigma_v^2$, which is the worst attainable distortion equivalent to simply estimating the source.

In the next section we show a scheme which is a combination of the schemes mentioned above, that for $I_\epsilon \neq 0$ gives both the optimal distortion for the designed SNR as well as a graceful degradation in distortion for all SNR's above the designed SNR. In the case of $I_\epsilon = 0$, or perfect secrecy, it is however not clear if we can get a graceful degradation in distortion.

2. Hybrid scheme using secrecy coding and vector quantization

In this scheme we quantize the source $\mathbf{v}$ to get $\mathbf{v}_q$ given as follows,

$$\mathbf{v} = \mathbf{v}_q + \mathbf{u}.$$

The quantized digital part is encoded using a secrecy code and the quantization error $\mathbf{u}$ is superimposed onto the secrecy code and transmitted with some scaling. The transmitted vector $\mathbf{x}$ is given by

$$\mathbf{x} = \mathbf{v}_{sec} + \kappa\mathbf{u}.$$

Here $\mathbf{v}_{sec}$ consists of a digital part that uses a secrecy code. The digital part $\mathbf{v}_{sec}$ uses a power of αP and the analog part a power of $(1-\alpha)P$. The source $\mathbf{v}$ is quantized to $\mathbf{v}_q$ at a rate $R(\alpha)$ chosen as

$$R(\alpha) = C\left(\frac{\alpha P}{(1-\alpha)P + \sigma^2}\right) - C\left(\frac{\alpha P}{(1-\alpha)P + \sigma_e^2}\right)$$

The encoder is the same encoder as in the Gaussian wire tap channel case [26] and [27]. We have $\approx 2^{NR(\alpha)}$ bins and $\approx 2^{NC\left(\frac{\alpha P}{(1-\alpha)P+\sigma_e^2}\right)}$ codewords in each bin. Hence the transmitted vector $\mathbf{v}_{sec}$ has a rate of $C\left(\frac{\alpha P}{(1-\alpha)P+\sigma^2}\right)$. The intended receiver can decode the digital part and cancel $\mathbf{v}_{sec}$ from $\mathbf{y}$. It then forms a minimum mean square estimate (MMSE) of $\mathbf{u}$. Hence the obtained distortion can be expressed as

$$D = \frac{\sigma_v^2 2^{-2R(\alpha)}}{1 + \frac{(1-\alpha)P}{\sigma_a^2}} \ .$$

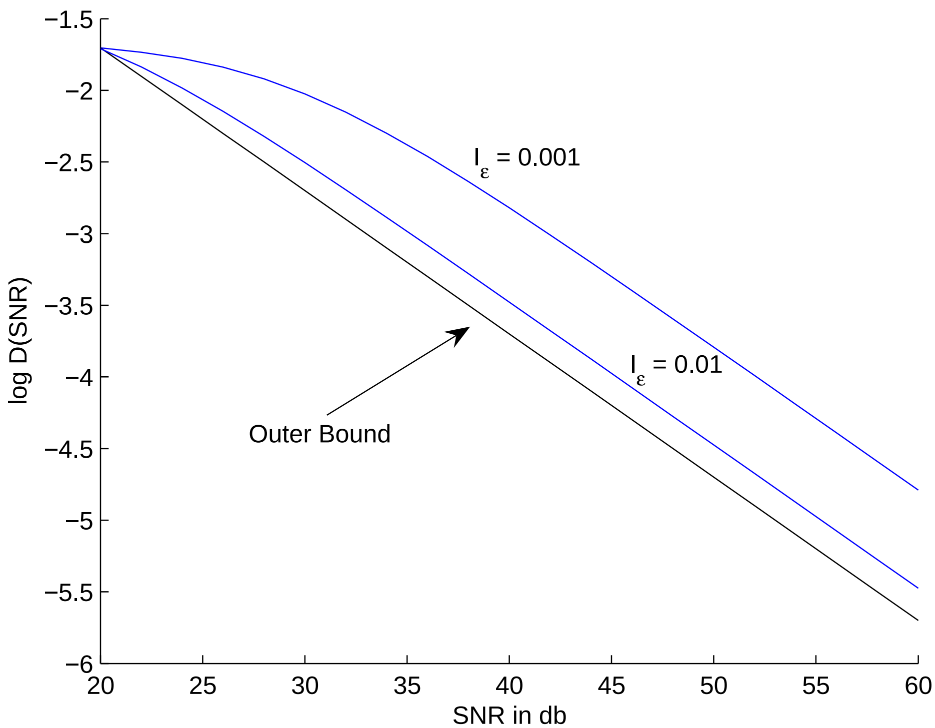

Fig. 14. Distortion vs SNR for different I_ϵ. Here $P = 1$, $\sigma^2 = 0.01(\mathsf{snr} = 20db)$ and $\sigma_e^2 = 1$.

The eavesdropper obtains $\mathbf{y}_e$ and we are interested in characterizing the information leakage rate I_ϵ. I_ϵ can be bounded as follows.

$$\begin{aligned}
I_\epsilon = \frac{1}{N} I(\mathbf{V};\mathbf{Y_e}) &\overset{(a)}{=} \frac{1}{N} I(\mathbf{V_q}, \kappa\mathbf{U};\mathbf{Y_e}) \\
&\overset{(b)}{=} \frac{1}{N} I(\mathbf{V_q};\mathbf{Y_e}) + \frac{1}{N} I(\kappa\mathbf{U};\mathbf{Y_e}|\mathbf{V_q}) \\
&\overset{(c)}{=} \frac{1}{N} I(\kappa\mathbf{U};\mathbf{Y_e}|\mathbf{V_q}) \\
&= \frac{1}{N} h(\kappa\mathbf{U}|\mathbf{V_q}) - \frac{1}{N} h(\kappa\mathbf{U}|\mathbf{Y_e}, \mathbf{V_q}) \\
&\overset{(d)}{\leq} \frac{1}{N} h(\kappa\mathbf{U}) - \frac{1}{N} h(\kappa\mathbf{U}|\mathbf{Y_e}, \mathbf{V_q}, \mathbf{V_{sec}}) \\
&\overset{(e)}{=} \frac{1}{N} h(\kappa\mathbf{U}) - \frac{1}{N} h(\kappa\mathbf{U} - \beta(\kappa\mathbf{U} + \mathbf{W_e})|\mathbf{Y_e}, \mathbf{V_q}, \mathbf{V_{sec}}) \\
&\overset{(f)}{=} \frac{1}{N} h(\kappa\mathbf{U}) - \frac{1}{N} h\left((1-\beta)\kappa\mathbf{U} - \beta\mathbf{W_e}\right) \\
&\overset{(g)}{=} \frac{1}{2} \log\left(1 + \frac{(1-\alpha)P}{\sigma_e^2}\right)
\end{aligned}$$

Here (a) follows because of the Markov chain $V \to (V_q, \kappa U) \to X$. (b) follows from the chain rule of mutual information. (c) is obtained by the choice of our coding scheme for $\mathbf{V_q}$, which is designed for perfect secrecy from the eavesdropper. Hence $H(\mathbf{V_q}|\mathbf{Y_e}) = H(\mathbf{V_q})$ or $I(\mathbf{V_q};\mathbf{Y_e}) = 0$. We obtain the first term in (d) since $\mathbf{V_q}$ is independent of $\mathbf{U}$, and the second term follows because conditioning reduces entropy. In (e), β is chosen as $\beta = \frac{(1-\alpha)P}{(1-\alpha)P+\sigma_e^2}$. (f) follows because $(1-\beta)\kappa\mathbf{U} - \beta\mathbf{W_e}$ is orthogonal to $\mathbf{Y_e}, \mathbf{V_q}$ and $\mathbf{V_{sec}}$ and finally (g) follows as all the terms are Gaussian. The distortion as a function of snr_a is plotted in Fig. 13 for $I_\epsilon = 0.01$, which shows that the hybrid scheme performs better than both the uncoded and the separation based scheme. Fig. 14 shows the performance of the hybrid scheme for different values of I_ϵ and this shows that the distortion exponent is -1 for $I_\epsilon > 0$. Also the distortion that can be achieved at the eavesdropper can be lower bounded by $\sigma_v^2 2^{-2I_\epsilon}$. This can be seen to be reasonably large when I_ϵ is small. Hence the eavesdropper gets only a poor estimate of the source.

A trivial outer bound for the problem can be obtained by assuming that the transmitter has knowledge of snr_a. [28] considers the rate distortion problem for the Shannon cipher system. It can be seen from [28, Theorem 1 with $R_k = 0$], that the Shannon cipher system reduces to the wire-tap channel setup and the optimal distortion can be achieved by separate source coding followed by secrecy coding. We first quantize the source $\mathbf{v}$ to $\mathbf{v_q}$ at a rate R. For a maximal leakage rate of I_ϵ, the maximum value of $R = C\left(\frac{P}{\sigma_a^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + I_\epsilon$. This can be obtained by following the steps outlined below.

Applying [27, Theorem 1, (2), (3) and (17)] to our problem setup we obtain the following set of equations.

$$R_v = \frac{H(\mathbf{V_q})}{n}$$

$$R_v \frac{H(\mathbf{V_q}|\mathbf{Y_e})}{H(\mathbf{V_q})} \leq C\left(\frac{P}{\sigma^2}\right) - C\left(\frac{P}{\sigma_e^2}\right)$$

The left hand side term can be simplified as follows,

$$\begin{aligned} R_v \frac{H(\mathbf{V_q}|\mathbf{Y_e})}{H(\mathbf{V_q})} &= R_v \frac{H(\mathbf{V_q}|\mathbf{Y_e}) - H(\mathbf{V_q}) + H(\mathbf{V_q})}{H(\mathbf{V_q})} \\ &\overset{(a)}{=} R_v \frac{H(\mathbf{V_q}) - nI_\epsilon}{H(\mathbf{V_q})} \\ &= R_v - I_\epsilon. \end{aligned}$$

In (a) we used the definition of I_ϵ. Thus we can bound R_v as,

$$R_v \leq C\left(\frac{P}{\sigma^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + I_\epsilon.$$

Hence the maximal rate R_v for the vector quantizer can be obtained by choosing $R_v = C\left(\frac{P}{\sigma^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + I_\epsilon$.

Hence we can achieve a distortion $D = \sigma_v^2 2^{-2R}$ corresponding to the above R. Fig. 14 shows the outer bound and we see that the achievable scheme has a constant gap from the outer bound.

E. JSCC for cognitive radio

Recently we observe a massive overcrowding of existing frequency spectrum by wireless devices [29, 30]. But there are many spectrum bands which are used very sparingly. This necessitates a need to find optimal use of the frequency bands. In this scenario, a cognitive transmitter and receiver, can make use of the unused spectrum without affecting the existing primary users. In this chapter we study the transmission and reconstruction of an analog source in a cognitive setting. Hybrid digital analog coding schemes considered in the previous chapter, can be seen as a natural choice for this cognitive setup. The problem model is schematically shown in the figure below.

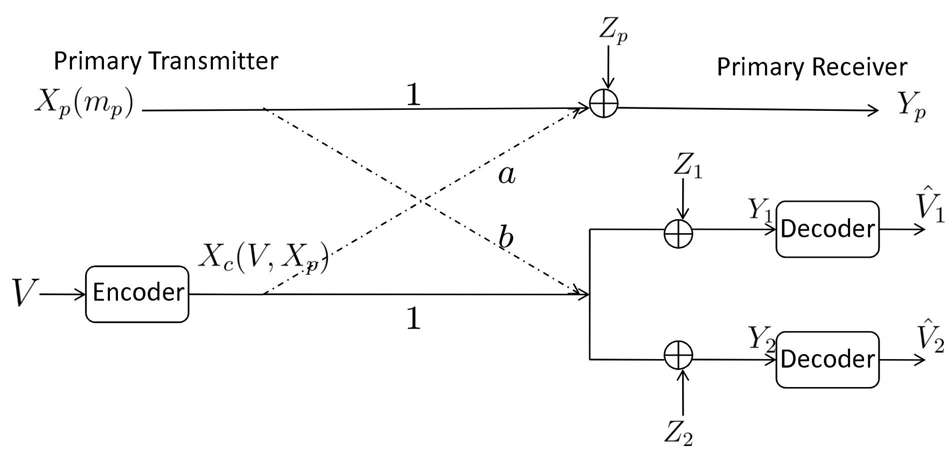

Fig. 15. Problem model for the cognitive setup.

We are interested in transmitting N symbols of an analog source V over N uses of a cognitive channel. We have a primary user and a cognitive user. The output vector of the primary user is given as $\mathbf{x_p}$. The cognitive user is assumed to know $\mathbf{x_p}$, the transmitted signal at the primary user. The transmitted vector at the cognitive user is $\mathbf{x_c}$ and is a function of V and $\mathbf{x_p}$. The cognitive user tries to transmit information to two/many cognitive receivers as shown in Fig. 15. The channel is modeled as an interference channel. The received vector $\mathbf{y_p}$ at the receivers can be expressed as

$$\mathbf{y_p} = \mathbf{x_p} + a\mathbf{x_c} + \mathbf{z_p}. \tag{3.7}$$

The received vector at the cognitive receivers 1 and 2 can be expressed as given below.

$$\mathbf{y_1} = \mathbf{x_c} + b\mathbf{x_p} + \mathbf{z_1}. \tag{3.8}$$

$$\mathbf{y_2} = \mathbf{x_c} + b\mathbf{x_p} + \mathbf{z_2}. \tag{3.9}$$

Z_1 and Z_2 are assumed to be zero mean Gaussian, with variance σ_1^2 and σ_2^2 respectively, with $\sigma_1^2 \geq \sigma_2^2$. The receivers reconstruct V as $\hat{V}_1$ and $\hat{V}_2$. The cognitive system has to be designed in such a manner, such that the primary user is not affected and gets its intended rate. We are hence interested in a characterization of the achievable distortion for the receiver with a better channel, when we design a scheme that is optimal for the receiver with the bad channel, for $a \leq 1$.

1. Achievable distortion for the HDA Costa coding scheme

The proposed scheme uses the idea of dirty paper coding applied to the analog setup. The cognitive transmitter has knowledge of the primary transmitters codeword, non-causally. The cognitive user by virtue of transmitting in the same spectrum, causes interference for the primary transmitter. However, the cognitive user can use part of its available power to transmit the primary message, and use the other part for it's intended cognitive receivers [31].

This can be expressed as

$$\mathbf{x_c} = \tilde{\mathbf{x}}_\mathbf{c} + \sqrt{\frac{\gamma P_c}{P_p}}\mathbf{x_p}. \tag{3.10}$$

The constant γ is chosen in a way, such that the capacity of the primary user is not compromised, while getting some non-zero information across for the cognitive users. The cognitive user does HDA costa coding as we have the setup of transmitting an analog source with interference $\mathbf{x_p}$, known only at the transmitter. The capacity of the primary user from (3.7)and (3.10) is then given by,

$$R_p = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_p} + a\sqrt{\gamma P_c})^2}{1 + a^2(1-\alpha)P_c}\right). \tag{3.11}$$

To satisfy the coexistence condition [31] i.e. the secondary transmitter does not degrade the performance of the primary user, we enforce that the primary user has the same capacity of $1/2\log(1+P_p)$. Hence we solve for γ, with $0 \le \gamma \le 1$, to satisfy

$$\frac{1}{2}\log\left(1 + P_p\right) = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_p} + a\sqrt{\gamma P_c})^2}{1 + a^2(1-\alpha)P_c}\right) \tag{3.12}$$

Solving the above equation gives the solution for γ^*.

Next we perform hybrid digital analog coding, following the same steps as in section II-B.2. We form an auxiliary random variable U, as follows

$$U = \tilde{X}_c + \alpha S + \kappa V. \tag{3.13}$$

Here S is a random variable given by, $S = \left(b + \sqrt{\frac{\gamma P_c}{P_p}}\right) X_p$. α and κ are constants given by

$$\alpha = \frac{\tilde{P}_c}{\tilde{P}_c + \sigma_1^2} \tag{3.14}$$

$$\kappa^2 = \frac{\tilde{P}_c^2}{(\tilde{P}_c + \sigma_1^2)\sigma_1^2}. \tag{3.15}$$

An $\mathbf{u}$ is found that is jointly typical with $\mathbf{s}$ and $\mathbf{v}$ and $\tilde{\mathbf{x}}_\mathbf{c}$ is transmitted along with the scaled version of $\mathbf{x_p}$. The receiver receives

$$\mathbf{y_1} = \mathbf{\tilde{x}_c} + \mathbf{s} + \mathbf{z_1} \tag{3.16}$$

From received $\mathbf{y_1}$, $\mathbf{u}$ is decoded and we obtain an estimate of $\mathbf{v}$ from both the decoded $\mathbf{u}$ and $\mathbf{y_1}$. This gives the distortion at the cognitive user as

$$D_1 = \frac{\sigma_v^2}{1 + \frac{(1-\alpha)P_c}{\sigma_1^2}} \tag{3.17}$$

The distortion achieved by the above scheme can also be obtained by a separation based scheme, involving a quantization of the source followed by digital Costa coding on the quantizer output bits.

The second user receives $\mathbf{y}_2 = \tilde{\mathbf{x}}_c + \mathbf{s} + \mathbf{z}_2$. Since the second user has a better channel than the first user, it can also decoder $\mathbf{u}$. The user then forms an MMSE estimate of $\mathbf{v}$ from $\mathbf{u}$ and $\mathbf{y}_2$. The distortion at the second user after algebraic manipulations can be obtained as

$$\begin{aligned} D_2 = &\left[(Q\sigma^4 + (\tilde{P}_c(\tilde{P}_c + Q) + 2\tilde{P}_c\sigma_1^2 + \sigma_1^4)\sigma_2^2)\sigma_v^2\right] \times \\ &\left[\tilde{P}_c^2(\tilde{P}_c + Q) + \tilde{P}_c(\tilde{P}_c + Q)\sigma_1^2 + Q\sigma_1^4 + (\tilde{P}_c(2\tilde{P}_c + Q) + 3\tilde{P}_c\sigma_1^2 + \sigma_1^4)\sigma_2^2\right]^{-1}. \end{aligned} \tag{3.18}$$

From the above expression, it can be seen that HDA coding provides and improvement in distortion performance than a digital Costa scheme, when the actual SNR is different from the design SNR.

F. Concluding remarks

In this chapter we considered several applications of JSCC. We studied the problem of broadcasting an analog source under bandwidth compression, and showed that a good scheme can be built for broadcasting by using HDA schemes. We also considered applications of JSCC for the cognitive setup. We also analyzed some JSCC schemes for transmitting an analog source in the presence of an eavesdropper. We showed that for a fixed information leakage to the eavesdropper I_ϵ, we can be both optimal for a design SNR and also obtain a graceful degradation of distortion with SNR. There are several problems of interest in this area, that can be studied as future work. One problem of interest is, whether it is still possible to obtain a graceful degradation of distortion, when we require perfect secrecy from the eavesdropper ($I_\epsilon = 0$). Another possible future work is the design of schemes for the source-channel bandwidth mismatch scenario, for both the cognitive setup and the secrecy setup.

CHAPTER IV

JOINT PHYSICAL LAYER CODING AND NETWORK CODING FOR BI-DIRECTIONAL RELAYING

In most modern systems physical layer coding and network layer coding are done separately. In this chapter, we show that significant throughput gains can be obtained by using a joint approach. Specifically, we consider a scenario where two users wish to exchange information with each other through a bi-directional relay. A separate physical layer coding followed by a network layer coding solution [4] for this problem is first presented. We show that a joint physical layer coding and network coding solution provides a significant increase in throughput when compared to the separation approach. We observe that structured lattice codes are very good candidates for this joint coding approach and they perform very close to the upper bound. For a comprehensive analysis, we study two types of decoding algorithms involving structured lattice codes in this chapter, namely a nested lattice decoding algorithm and a minimum angle decoding algorithm, and we evaluate the performance of each of these algorithms. We next present the detailed system model.

A. System model and problem statement

We study the Gaussian version of the two-way relay problem considered in [4]. More specifically, we study a simple 3-node linear Gaussian network as shown in Fig. 16. Nodes A and B wish to exchange information between each other through the relay node J, however, nodes A and B cannot communicate with each other directly. Let $\mathbf{u}_1 \in \{0,1\}^k$ and $\mathbf{u}_2 \in \{0,1\}^k$, be the information vectors at nodes A and B. The information is assumed to be encoded into vectors (codewords) $\mathbf{x}_1 \in \mathbb{R}^n$ and $\mathbf{x}_2 \in \mathbb{R}^n$ at nodes A and B, respectively, and transmitted. We assume that communication takes place in two phases - a multiple access (MAC) phase and a broadcast phase, which are briefly described below.

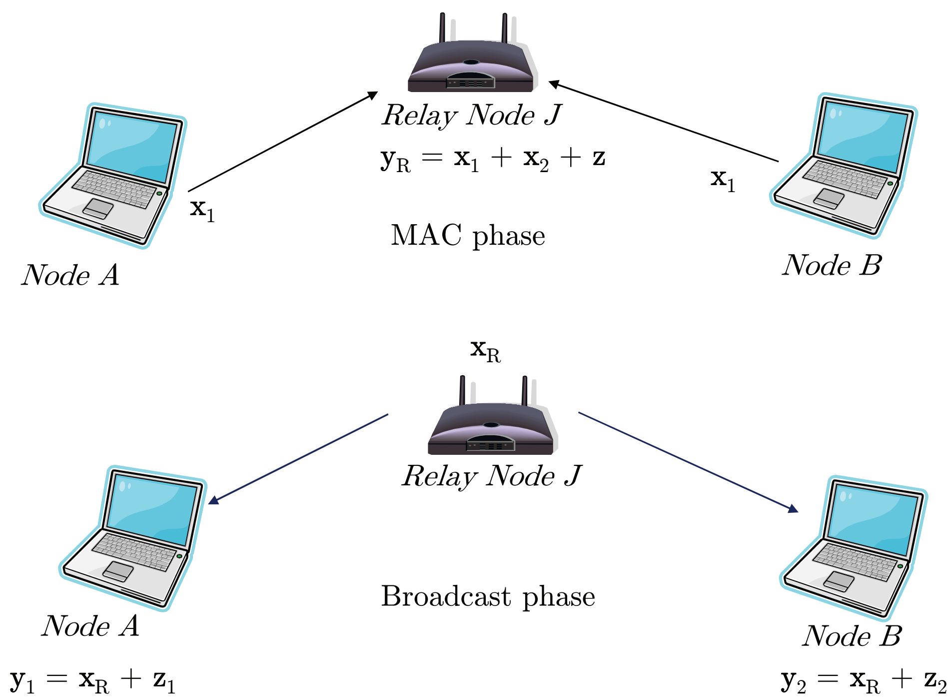

Fig. 16. System model with 3 nodes.

MAC phase: During the MAC phase, nodes A and B transmit $\mathbf{x}_1$ and $\mathbf{x}_2$ in n uses of an AWGN channel to the relay. It is assumed that the two transmissions are perfectly synchronized and, hence, the received signal at the relay $\mathbf{y}_R \in \mathbb{R}^n$ is given by

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

where the components of $\mathbf{z}$ are independent identically distributed (i.i.d) Gaussian random variables with zero mean and variance σ^2. Further, it is assumed that there is an average transmit power constraint of P at both nodes and, hence, $E[||\mathbf{x}_1||^2] \leq nP$ and $E[||\mathbf{x}_2||^2] \leq nP$.

Broadcast phase: During the broadcast phase, the relay node transmits $\mathbf{x}_R \in \mathbb{R}^n$ in n uses of an AWGN broadcast channel to both nodes A and B. It is assumed that the average transmit power at the relay node is also constrained to P and that the noise variance at the two nodes is also σ^2. Node A forms an estimate of $\mathbf{u}_2$, namely $\hat{\mathbf{u}}_2$ and node B forms an estimate of $\mathbf{u}_1$, namely $\hat{\mathbf{u}}_1$. An error is said to occur if either $\mathbf{u}_2 \neq \hat{\mathbf{u}}_2$ or $\mathbf{u}_1 \neq \hat{\mathbf{u}}_1$, i.e., the probability of error is given by

$$P_e \triangleq \Pr\left(\{\mathbf{u}_1 \neq \hat{\mathbf{u}}_1\} \bigcup \{\mathbf{u}_2 \neq \hat{\mathbf{u}}_2\}\right).$$

It is assumed that the communications in the MAC and broadcast phases are orthogonal and each phase uses the channel exactly n times. For example, the communications in the MAC and broadcast phase could be in two separate frequency bands (or in two different time slots) and, hence, the MAC phase and broadcast phase do not interfere with each other. To keep the discussion simple, we will assume that the MAC and broadcast phases occur in different time slots. This can be easily generalized to the case when $2n$ dimensions are available for communication, out of which n dimensions are allocated to the MAC phase and n dimensions are allocated to the broadcast phase. Note that the signal-to-noise ratio (SNR) for all transmissions is $\mathsf{snr} = P/\sigma^2$ and, hence, we refer to it as simply the SNR without having to distinguish between the SNRs of the different phases. Similarly, we restrict our attention to the symmetric rate case when both the nodes A and B wish to exchange identical amount of information and, hence, we can simply refer to one exchange rate without having to distinguish between the rate for A and B separately.

For a given encoding/decoding scheme, we say that the rate R_{scheme} is achievable if, for any $\epsilon > 0$ and for every n sufficiently large, there exists a k, such that $\frac{k}{n} > R_{scheme}$ and $P_e < \epsilon$. The exchange capacity C_{ex} is then the supremum of R_{scheme} over all possible encoding/decoding schemes.

B. Main results and comments

The main results in this chapter are,

- An upper bound on the exchange capacity is given by

$$C_{ex} \leq \frac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right).$$

- *Lattice decoding:* A dithered nested lattice encoding scheme with nested lattice decoding discussed in section F achieves an exchange rate of

$$R_{Lattice} = \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right).$$

- *Minimum angle decoding:* A scheme using lattice encoding (without dither) and minimum angle decoding discussed in Section G also achieves the same exchange rate of

$$R_{Lattice} = \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right).$$

At high SNRs, the lattice based coding and decoding schemes are nearly optimal because their rate approach the upper bound.

C. Related prior work

Recently, there has been a significant amount of work on coding for the bi-directional relay problem [4, 32–38]. In [4], Katti *et al.*, showed the usefulness of network coding for this problem. Although they do not consider the physical layer explicitly, the natural extension of their solution to our problem would work as follows. The $2n$ channel uses available for signaling would be split into three slots with $2n/3$ channel uses each. In the first time slot, $\mathbf{u}_1$ is encoded using an optimal channel code for the AWGN channel into $\mathbf{x}_1$ and transmitted from node A. Similarly, in the second time slot $\mathbf{u}_2$ is encoded into $\mathbf{x}_2$ and transmitted from node B. At the relay, $\mathbf{u}_1$ and $\mathbf{u}_2$ are decoded and then the relay forms $\mathbf{u}_R = \mathbf{u}_1 \oplus \mathbf{u}_2$ and encodes $\mathbf{u}_R$ into $\mathbf{x}_R$ using an optimal code for the Gaussian channel and broadcasts to both nodes. The two nodes decode $\mathbf{u}_R$ and then since they have $\mathbf{u}_1$ and $\mathbf{u}_2$, they can obtain $\mathbf{u}_2$ and $\mathbf{u}_1$ at the nodes A and B, respectively. Here, the physical layer and network layer are completely separated and coding (or mixing of the information) is performed only at the network layer. In the system model considered in Fig. 16, the physical layer naturally performs mixing of the signals from the two transmitters. The schemes that take advantage of this can be referred to as joint physical layer coding and network coding solutions.

One such scheme called analog network coding was proposed in [33]. In this case, the MAC phase and broadcast phase use n uses of the AWGN and are orthogonal to each other. Gaussian code books are used at the transmitters to encode $\mathbf{u}_1$ into $\mathbf{x}_1$ and $\mathbf{u}_2$ into $\mathbf{x}_2$, respectively. Analog network coding is an amplify and forward scheme where the received signal at the relay during the MAC phase $\mathbf{y}_R$, is scaled to satisfy the power constraint and transmitted during the broadcast phase, i.e., $\mathbf{x}_R = \sqrt{\frac{P}{2P+\sigma^2}}\mathbf{y}_R$. It can be seen that this scheme can achieve an exchange rate of $\frac{1}{2}\log\left(1 + \frac{P}{3P+\sigma^2}\frac{P}{\sigma^2}\right)$, which is higher than that achievable with the pure network coding scheme in [4] for high SNR.

The scheme proposed in this paper can be thought of as a decode and forward scheme. This scheme outperforms the amplify and forward scheme in [33]. In [36], it is conjectured that an exchange rate of $\frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$ can be achieved, however, no scheme is given. The scheme in this paper is a constructive scheme that performs close to the rate conjectured in [36]. The lattice decoding scheme discussed in Section F is similar to that used by Nazer and Gastpar [39] for the problem of estimating the sum of two Gaussian random variables, but was independently proposed in the conference version of this chapter [40]. Several other schemes have also been recently suggested for bi-directional relaying. In [41], Kim et. al. introduced compress-forward and mixed-forward schemes for bi-directional relaying with asymmetric channel gains. These schemes use random codes instead of structured codes. In a very recent work [42], which appeared after the publication of our work in [40], Nam et. al. introduced nested lattice codes for the same problem. In their scheme, which is optimal at high SNR, each node uses a lattice with a different rate and nested lattice decoding is performed at the relay.

D. An optimal transmission scheme for the BSC channel

To motivate our proposed scheme, we first consider a system where the physical layer channels are all binary symmetric channels. i.e., $\mathbf{x}_1 \in \{0,1\}^n$, $\mathbf{x}_2 \in \{0,1\}^n$ and the signal received at the relay is

$$\mathbf{y}_R = \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{e}, \tag{4.1}$$

where $\oplus$ denotes binary addition and $\mathbf{e}$ is an error sequence whose components are 0 or 1 with probability q and $1-q$ respectively and are i.i.d. Similarly, during the broadcast phase, let the channel be a BSC channel with crossover probability q. In this case, an upper bound on the exchange capacity is $1 - H(q)$ since this is the maximum information that can flow to any of the nodes from the relay. This can be achieved using the following coding scheme.

In this scheme, the two nodes transmit using identical capacity achieving binary *linear* codes of rate $1 - H(q)$. Consider again the received signal at the relay given in (4.1). Notice that since $\mathbf{x}_1$ and $\mathbf{x}_2$ are codewords from the same linear code, $\mathbf{x}_1 \oplus \mathbf{x}_2$ is also a valid codeword from the same code which achieves capacity over a BSC channel with crossover probability q. Hence, the relay can decode $\mathbf{x}_1 \oplus \mathbf{x}_2$ and transmit the result during the broadcast phase. The nodes A and B can also decode $\mathbf{x}_1 \oplus \mathbf{x}_2$ and since they have $\mathbf{x}_1$ and $\mathbf{x}_2$, they can obtain $\mathbf{x}_2$ and $\mathbf{x}_1$, respectively. This scheme achieves an exchange rate of $1 - H(q)$ and is therefore optimal.

Random codes versus structured codes: It is quite interesting to note that if random codes, i.e., codes from the Shannon ensemble were used instead of linear codes, $\mathbf{x}_1 \oplus \mathbf{x}_2$ cannot be decoded at the relay. The linearity (or group structure) of the code is exploited to make $\mathbf{x}_1 \oplus \mathbf{x}_2$ decodable at the relay and, hence, structured codes with a group structure outperform random codes for this problem. Examples of schemes where structured codes outperform random codes have been given in Korner and Marton [43] and more recently by Nazer and Gastpar in [44, 45].

E. Upper bound on the exchange rate for Gaussian links

Let us now return to the problem outlined in Section A, where the channels between the nodes and the relay are AWGN channels. We restrict our attention to schemes where the MAC phase and broadcast phase are both orthogonal to each other and use n channel uses (or dimensions). With this restriction, a simple upper bound on the exchange rate can be obtained as follows. Consider a cut between the relay node and node A. The maximum amount of information that can flow to either of the nodes from the relay is $\frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$. Hence, the exchange capacity is upper bounded by

$$C_{ub} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right).$$

We next consider coding schemes and analyze their performance.

F. Nested lattice based coding scheme with lattice decoding

As shown in section D for the BSC channel, codes with a group structure (linear codes) enable decoding of a linear combination (or, sum) of codewords at the relay. This motivates the use of lattice codes for the Gaussian channel since lattices have a similar group structure with respect to real vector addition. We begin with some preliminaries about lattices [13, 46].

An n-dimensional lattice Λ is a subgroup of $\mathbb{R}^n$ under vector addition over the reals. This implies that if $\lambda_1, \lambda_2 \in \Lambda$, then $\lambda_1 + \lambda_2 \in \Lambda$. For any $\mathbf{x} \in \mathbb{R}^n$, the quantization of $\mathbf{x}$, $Q_\Lambda(\mathbf{x})$ is defined as the $\lambda \in \Lambda$ that is closest to $\mathbf{x}$ with respect to Euclidean distance. The fundamental Voronoi region $\mathcal{V}(\Lambda)$ is defined as $\mathcal{V}(\Lambda) = \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$. The mod operation is defined as $(\mathbf{x} \mod \Lambda) = \mathbf{x} - Q_\Lambda(\mathbf{x})$. This can be interpreted as the error in quantizing an $\mathbf{x}$ to the closest point in the lattice Λ. The second moment of a lattice is given by

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

and where $V(\Lambda)$, the volume of the fundamental Voronoi region is denoted by $V(\Lambda) = \int_{\mathcal{V}(\Lambda)} d\mathbf{x}$. The normalized second moment of the lattice is then given by

$$G(\Lambda) = \sigma^2(\Lambda)/V(\Lambda)^{2/n}.$$

Let us define the covering radius of a lattice $\mathcal{R}_u$ as the radius of the smallest n-dimensional hypersphere containing the Voronoi region $\mathcal{V}(\Lambda)$. Also let $\mathcal{R}_l$ denote the effective radius of $\mathcal{V}(\Lambda)$, which is the radius of the n-dimensional hypersphere having the same volume as $\mathcal{V}(\Lambda)$. Now we can define a Rogers-good Lattice [46, (69)] as a lattice that satisfies

$$1 \leq \left(\frac{\mathcal{R}_u}{\mathcal{R}_l}\right)^n < c \cdot n \cdot (\log n)^a, \tag{4.2}$$

where c and a are positive constants. This implies,

$$\frac{1}{n} \log \frac{\mathcal{R}_u}{\mathcal{R}_l} = \mathcal{O}\left(\frac{1}{n}\right). \tag{4.3}$$

We next define nested lattices. Formally, we say that the lattice Λ_c (the coarse lattice) is nested in the lattice Λ_f (the fine lattice) if $\Lambda_c \subseteq \Lambda_f$ [47]. Let the fundamental Voronoi regions of the lattices, Λ_c and Λ_f be $\mathcal{V}(\Lambda_c)$ and $\mathcal{V}(\Lambda_f)$. In this work, we are interested in nested lattices as they can be easily adapted to the AWGN channel, with the fundamental Voronoi region of the coarse lattice $\mathcal{V}(\Lambda_c)$ acting as a power constraint and fine lattice points of Λ_f in $\mathcal{V}(\Lambda_c)$ acting as the codewords. The number of lattice points of the fine lattice in $\mathcal{V}(\Lambda_c)$ is given by the nesting ratio $\frac{V(\Lambda_c)}{V(\Lambda_f)}$. The coding rate, $R_{Lattice}$ of the nested lattice code captures the rate of the nested lattice code, and is defined as the logarithm of the number of lattice points of the fine lattice in $\Lambda_f \cap \mathcal{V}(\Lambda_c)$ given by

$$R_{Lattice} = \frac{1}{n} \log |\Lambda_f \cap \mathcal{V}(\Lambda_c)| = \frac{1}{n} \log \frac{V(\Lambda_c)}{V(\Lambda_f)}.$$

Lattice codes can be used to achieve capacity on the single user AWGN channel under maximum likelihood (ML) decoding [48–50]. The initial work [48], had an error and was corrected by [49]. ML decoding requires finding the lattice point inside a spherical bounding region(serves as a power constraint), which is closest to the received signal. In contrast, lattice decoding ignores the bounding region and finds the closest lattice point to the received signal. Lattice decoding has a much lower complexity than ML decoding and has hence attracted a lot of interest. More recently, nested lattices have been shown to achieve the capacity of the single user AWGN

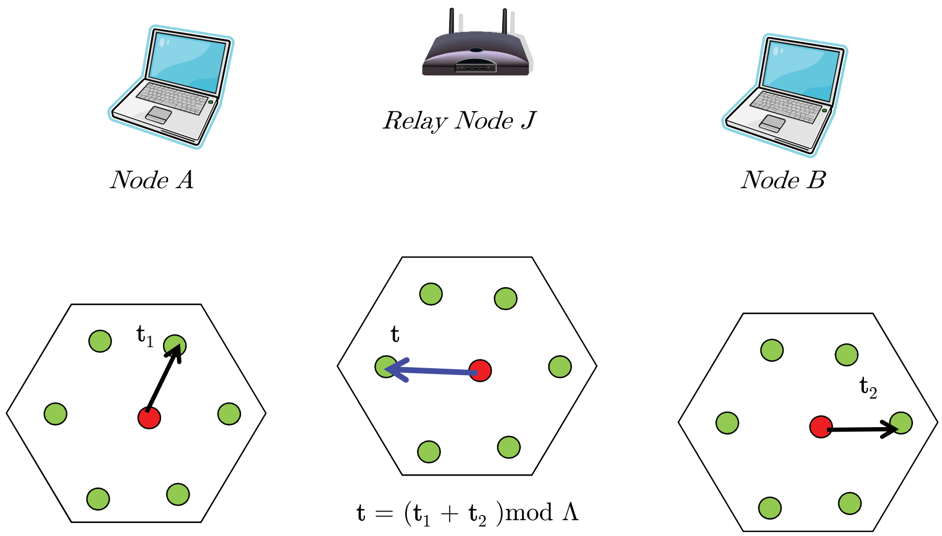

Fig. 17. Lattice coding based scheme showing the transmitted signals $\mathbf{t}_1$, $\mathbf{t}_2$ and the decoded signal at the relay $\mathbf{t}$.

channel under lattice decoding [13, 46]. The main idea in [13, 46] is to use the coarse lattice as a shaping region and the lattice points from the fine lattice contained within the basic Voronoi region of the coarse lattice as the codewords. The existence of *"good"* nested lattices whose coarse lattice Λ_c is simultaneously Rogers-good(good for quantization) and Poltyrev-good (good for channel coding [46, eqn. (78)]), and fine lattice is Poltyrev-good has been shown in [46]. It is also shown in [46] that the choice of such a nested lattice achieves the AWGN channel capacity, under lattice decoding.

1. Description and achievable rate

We now describe our encoding and decoding schemes for the bi-directional relaying problem using nested lattices. The encoding and decoding operations during the MAC and broadcast phase are explained below. A general schematic is also shown in Fig. 17.

MAC Phase:

Let there be k information bits in the information vector $\mathbf{u}_1$ and $\mathbf{u}_2$ and, hence, the exchange rate is $R_{Lattice} = k/n$. At node A, the information vector $\mathbf{u}_1$ is mapped onto a fine lattice point $\mathbf{t}_1 \in \{\Lambda_f \cap \mathcal{V}(\Lambda_c)\}$, i.e., the set of all fine lattice points in the basic Voronoi region of the coarse lattice is taken to be the code. An identical code is used at node B and the information vector $\mathbf{u}_2$ is mapped onto the codeword $\mathbf{t}_2 \in \{\Lambda_f \cap \mathcal{V}(\Lambda_c)\}$. We then generate dither vectors $\mathbf{d}_1$ and $\mathbf{d}_2$ which are randomly generated n dimensional vectors uniformly distributed over $\mathcal{V}(\Lambda_c)$. The dither vectors are mutually independent of each other and are known at both the relay node and the nodes A and B. Now node A and node B form the transmitted signals $\mathbf{x}_1$ and $\mathbf{x}_2$ as follows

$$\mathbf{x}_1 = (\mathbf{t}_1 - \mathbf{d}_1) \mod \Lambda_c \tag{4.4}$$

$$\mathbf{x}_2 = (\mathbf{t}_2 - \mathbf{d}_2) \mod \Lambda_c. \tag{4.5}$$

By choosing an appropriate coarse lattice Λ_c with second moment P, the transmit power constraint will be satisfied at both nodes. The relay node receives $\mathbf{y}_R$ given by

$$\mathbf{y}_R = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z}, \tag{4.6}$$

where $\mathbf{z}$ is the noise vector whose components have variance σ^2.

At the decoder, the relay attempts to decode to $\mathbf{t} \triangleq (\mathbf{t}_1 + \mathbf{t}_2) \mod \Lambda_c$ from the received signal $\mathbf{y}_R$. The decoder at the relay node first forms

$$\hat{\mathbf{t}} = (\alpha \mathbf{y}_R + \mathbf{d}_1 + \mathbf{d}_2) \mod \Lambda_c,$$

where α is a constant given by $\alpha = \frac{2P}{2P+\sigma^2}$. The relay next attempts to decode to $\mathbf{t}$ by finding the lattice point closest to $\hat{\mathbf{t}}$, i.e., the estimate of $\mathbf{t}$ is $Q_{\Lambda_f}(\hat{\mathbf{t}})$. The decoding is then successful if $\mathbf{t} = Q_{\Lambda_f}(\hat{\mathbf{t}})$. The detailed steps in decoding to $\mathbf{t}$ with arbitrarily low probability of error is given below.

Analysis of the probability of error of the nested lattice decoder: We first show that $\hat{\mathbf{t}}$ can be expressed as the output of an equivalent modulo-lattice additive noise (MLAN) channel. Using the distributive property of the mod operation, i.e., $\{\mathbf{x} \mod \Lambda + \mathbf{y} \mod \Lambda\} \mod \Lambda = \{(\mathbf{x}+\mathbf{y}) \mod \Lambda\} \mod \Lambda$, $\hat{\mathbf{t}}$ can be written as:

$$
\begin{aligned}
\hat{\mathbf{t}} &= (\alpha \mathbf{y}_R + \mathbf{d}_1 + \mathbf{d}_2) \mod \Lambda_c \\
&= (\alpha(\mathbf{x}_1 + \mathbf{x}_2) + \alpha \mathbf{z} + \mathbf{d}_1 + \mathbf{d}_2) \mod \Lambda_c \\
&= (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{d}_1 + \mathbf{d}_2 + \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)) \mod \Lambda_c \\
&= ((\mathbf{t}_1 - \mathbf{d}_1) \mod \Lambda_c + (\mathbf{t}_2 - \mathbf{d}_2) \mod \Lambda_c + \mathbf{d}_1 + \mathbf{d}_2 + \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)) \mod \Lambda_c \\
&\overset{(a)}{=} ((\mathbf{t}_1 + \mathbf{t}_2) \mod \Lambda_c + \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)) \mod \Lambda_c \\
&\overset{(b)}{=} (\mathbf{t} + \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)) \mod \Lambda_c \\
&\overset{(c)}{=} \mathbf{t} + \mathbf{z}_{eq} \mod \Lambda_c.
\end{aligned} \tag{4.7}
$$

Here, (a) follows from the distributive property of the $\mod \Lambda_c$ operation. (b) follows from the definition of $\mathbf{t}$ and in (c), we define $\mathbf{z}_{eq}$ as $\mathbf{z}_{eq} \triangleq \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)$. The relay can decode to $\mathbf{t}$, if $Q_{\Lambda_f}(\hat{\mathbf{t}}) = \mathbf{t}$.

Due to the group structure of the lattice, $\mathbf{t}$ is a lattice point in the fine lattice (more precisely, $\mathbf{t} \in \{\Lambda_f \cap \mathcal{V}(\Lambda_c)\}$). By applying the *crypto lemma* [51], it can be seen that $\mathbf{t}$ is uniformly distributed over the fine lattice points in $\mathcal{V}(\Lambda_c)$. Further, note that $\mathbf{t}_1$ and $\mathbf{t}_2$ are independent of $\mathbf{z}$, $\mathbf{x}_1$ and $\mathbf{x}_2$ and, hence, we can define an equivalent noise term $\mathbf{z}_{eq} = \alpha \mathbf{z} - (1-\alpha)(\mathbf{x}_1 + \mathbf{x}_2)$ such that $\mathbf{t}$ and $\mathbf{z}_{eq}$ are independent of each other. The second moment of Z_{eq} is given by $\sigma_{eq}^2 = E[Z_{eq}^2] = \alpha^2\sigma^2 + (1-\alpha)^2 2P$. We can now choose α to minimize $E[z_{eq}^2]$ and the resulting optimum values of α and σ_{eq}^2 are $\alpha_{opt} = \frac{2P}{2P+\sigma^2}$ and $\sigma_{eq,opt}^2 = \frac{2P\sigma^2}{2P+\sigma^2}$, respectively. Also, $\alpha \mathbf{y}_R$ can be treated as a linear estimate of $(\mathbf{x}_1 + \mathbf{x}_2)$. For a detailed discussion on using linear estimation for nested lattice decoding, see [46, section V]. The following theorem establishes that it is possible to decode to $\mathbf{t}$ with arbitrarily low probability of error, if the coding rate of the lattice is $< \frac{1}{2}\log\left(\frac{P}{\sigma_{eq}^2}\right) = \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right)$, where P is the second moment per dimension of the coarse lattice.

Theorem F.1 (modified version of [46, Theorem 5])**.** *For any coding rate $R_{Lattice} < \frac{1}{2}\log(\frac{1}{2}+\frac{P}{\sigma^2})$, there exists a sequence of n-dimensional nested lattice pairs $(\Lambda_f^{(n)}, \Lambda_c^{(n)})$ of coding rate $R_{Lattice}$ for which*

$$\Pr\{\mathbf{Z}_{eq} \notin \mathcal{V}(\Lambda_f^{(n)})\} \to 0, \ \textit{as } n \to \infty,$$

where $\mathbf{z}_{eq} = (1-\alpha)(\mathbf{x}_1+\mathbf{x}_2)+\alpha\mathbf{z}$ and $\alpha = \frac{2P}{2P+\sigma^2}$. Here $\mathbf{x}_1$ and $\mathbf{x}_2$ are realizations of two independent random variables uniformly distributed over $\mathcal{V}(\Lambda_c^{(n)})$ and $\mathbf{z}$ is a realization of an n-dimensional Gaussian vector $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$, where $\mathbf{I}$ is an $n \times n$ identity matrix. Also the coarse lattice $\Lambda_c^{(n)}$ has a maximum second moment(per dimension) of P.

Proof. The proof follows closely the proof of [46, Theorem 5]. The main idea is to show that $\mathbf{Z}_{eq}$ can be well approximated by a Gaussian distribution with nearly the same variance, and show that the approximation gets better as $n \to \infty$. We mention below the places where the proof in [46] have to be modified. [46, eqn. 81] must be changed to take into account that we have two transmitters. [46, eqn. 81] must be modified with Lemma J.1 given in appendix J.1. Also [46, eqn. 82] must be modified with Lemma J.2 stated in appendix J.1. After this, we can continue with the proof in [46] by calculating the Poltyrev exponents [52] and also using the fact that Rogers-good and Poltyrev-good [46, pg. 2306] lattices exist. Continuing with these steps in [46] shows that any rate of $R_{Lattice} < \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right)$ for which $\Pr\{\mathbf{Z}_{eq} \notin \mathcal{V}(\Lambda_f^{(n)})\} \to 0, \ \text{as } n \to \infty$, can be obtained. This proves the theorem. $\square$

The probability distribution of the $n-$dimensional noise vector $\mathbf{Z}_{eq}$ considered in theorem F.1 is slightly different from the noise distribution in [46, Theorem 5], and we can not directly apply [46, Theorem 5] to our case. Hence, we had to show that $\mathbf{Z}_{eq}$ is similar to a Gaussian distribution at high dimensions, and also show the existence of good lattices with rates that approach the proposed coding rates.

Broadcast phase:

In the broadcast phase, the relay node transmits the index of $\mathbf{t}$ using a capacity achieving code for the AWGN channel. Since the capacity of the AWGN channel is $\frac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right)$ which is higher than $R_{Lattice}$ from theorem F.1 and, hence, the index (or, equivalently, $\mathbf{t}$) can be obtained at the nodes A and B. Since node A already has $\mathbf{u}_1$ and, hence, $\mathbf{t}_1$, it needs to recover $\mathbf{u}_2$ or, equivalently, $\mathbf{t}_2$, from $\mathbf{t}$ and $\mathbf{t}_1$. This can be done as follows. Node A computes $(\mathbf{t}-\mathbf{t}_1) \mod \Lambda_c$, which can be written as

$$(\mathbf{t}-\mathbf{t}_1) \mod \Lambda_c = ((\mathbf{t}_1+\mathbf{t}_2) \mod \Lambda_c - \mathbf{t}_1) \mod \Lambda_c = \mathbf{t}_2 \mod \Lambda_c = \mathbf{t}_2. \quad (4.8)$$

Similarly, $\mathbf{t}_1$ can also be obtained at node B by computing $(\mathbf{t}-\mathbf{t}_2) \mod \Lambda_c$. Hence, an effective exchange rate of $R_{Lattice} < \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right)$ can be obtained using nested lattices with lattice decoding.

We conclude by noting that, at high SNR, this scheme approaches the upper bound of $\frac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right)$ and is therefore nearly optimal. This scheme can be interpreted as a Slepian-Wolf coding scheme using nested lattices, i.e., the relay wishes to convey $(\mathbf{t}_1+\mathbf{t}_2) \mod \Lambda_c$ to node A, where some side information (namely, $\mathbf{t}_1$) is available. Thus, the broadcast phase in effect uses nested lattices for solving the Slepian-Wolf coding problem. This scheme can also be thought of as a decode and forward scheme where the relay decodes a function of $\mathbf{t}_1$ and $\mathbf{t}_2$, namely $\mathbf{t} = (\mathbf{t}_1+\mathbf{t}_2) \mod \Lambda_c$ and forwards this to the nodes. Notice however, that the relay will not know either $\mathbf{t}_1$ or $\mathbf{t}_2$ exactly, it only knows $\mathbf{t}$.

Since the nested lattice code used is by itself a capacity achieving code for the AWGN channel, one does not have to encode $\mathbf{t}$ again using a separate capacity achieving channel code. The relay can simply broadcast $\mathbf{x}_R = (\mathbf{t} - \mathbf{d}) \mod \Lambda_c$, where $\mathbf{d}$ is an uniform dither. Notice that $E[||\mathbf{x}_R||^2] \leq P$ and, hence, the power constraint will be satisfied at the relay node and $\mathbf{t}$ can be decoded at the nodes A and B by nested lattice decoding.

G. Lattice coding with minimum angle decoding

In the previous section we observed that nested lattice decoding can achieve an exchange rate of $\frac{1}{2}\log(\frac{1}{2} + \frac{P}{\sigma^2})$ with lattice decoding alone, and does not attain the upper bound $\frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$. This naturally leads us to the question - is the upper bound loose or is the nested lattice coding scheme with lattice decoding suboptimal? Particularly, we are interested in investigating whether the fact that we decode to the modulo-Λ_c sum of codewords at the relay and the use of two independent dithers (resulting in two independent self-noise) is suboptimal. Hence, we are interested in studying another encoding/decoding scheme. Let us consider the set of all $\mathbf{x}_{sum}$'s, where $\mathbf{x}_{sum} \triangleq \mathbf{x}_1 + \mathbf{x}_2$, and $\mathbf{x}_1$ and $\mathbf{x}_2$ are the codewords/lattice points transmitted from nodes A and B, respectively. Ideally the optimal decoder for decoding to the $\mathbf{x}_{sum}$'s is the maximum a posteriori(MAP) decoder. However, the MAP decoder is difficult to analyze and, hence, we study a suboptimal minimum angle decoder [50]. The analysis of this minimum angle decoder is also insightful in understanding the geometry of the codebook induced by the addition of two lattice points at the relay. Our analysis in this section shows that the suboptimal angle decoder achieves an exchange rate of $\frac{1}{2}\log(\frac{1}{2} + \frac{P}{\sigma^2})$. Though, we have not adequately answered the question of whether the upper bound is tight, the analysis of the minimum angle decoder scheme shows that one cannot simply replace lattice decoding by minimum angle decoding in order to obtain better rates.

1. Description

We now describe the proposed lattice coding scheme with minimum angle decoding at the relay. We consider an n-dimensional lattice $\Lambda_n \subset \mathbb{R}^n$. Let $T_{\sqrt{P}}$ be an n-dimensional closed ball, centered at the origin and having a radius $\sqrt{nP}$, and let $V_n(\sqrt{nP})$ be the hypervolume of $T_{\sqrt{P}}$. This can be treated as a power constraint. Our codewords will be composed of lattice points in the sphere $T_{\sqrt{P}}$. Each transmitter chooses a lattice point corresponding to its message index and transmits synchronously over the Gaussian channel. Here we have no nested lattice construction or the use of an explicit random dither in the encoding stage. However, we will have a fixed lattice translation that serves a similar role as that of a dither. At the receiver we will be interested in decoding to the actual sum of these lattice points, without the modulo operation.

Minimum angle decoder: A minimum angle decoder discussed here makes a decision based on lattice points in a thin n-dimensional spherical shell $T^{\Delta}_{\sqrt{2P}} \triangleq \{\mathbf{x} \in \mathbb{R}^n : \sqrt{n(2P-\delta)} \leq \|\mathbf{x}\| \leq \sqrt{n(2P+\delta)}\}$, δ is small and non-zero. It takes the received vector and finds the lattice point, whose projection on the thin shell, is closest to the received vector.

During the broadcast phase the relay performs Slepian-Wolf coding which is explained in section G.4.

We now state the main theorem of this section.

Theorem G.1. *For the bi-directional relaying problem considered in Section A, there* *exists at least one n-dimensional lattice Λ_n^* such that any exchange rate of $R_{Lattice} < \frac{1}{2}\log(\frac{1}{2} + SNR)$ is achievable using a minimum angle decoder as $n \to \infty$.*

The proof of the above theorem is tedious. Therefore, we first present a proof sketch for the achievable lattice coding rate during the MAC phase in section G.2 which outlines the main ideas in the proof. Then, a detailed proof is given in section G.3. The broadcast scheme required for the proof of the above theorem is presented in G.4.

2. Proof sketch for MAC phase

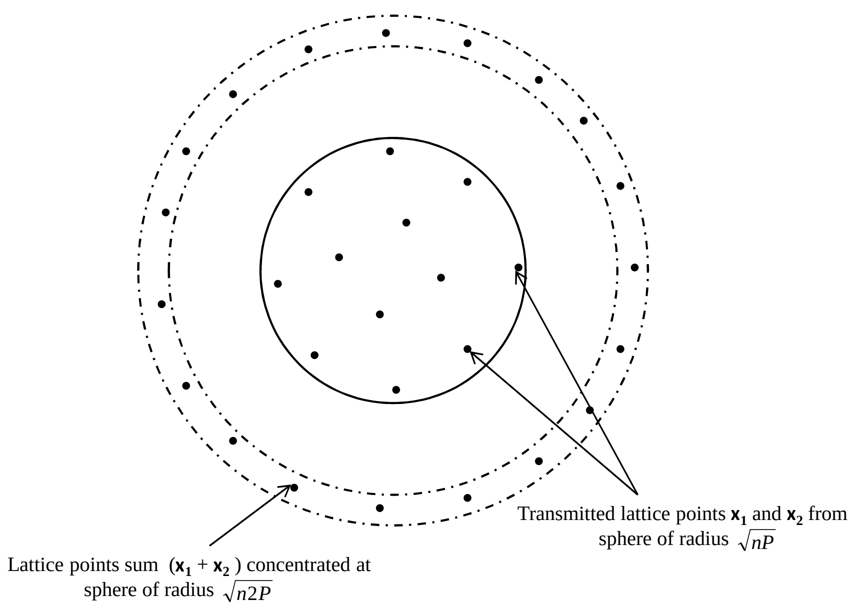

Fig. 18. Picture showing the concentration of the sum of lattice points on the thin shell of radius $\sqrt{n2P}$.

It is well known that the volume of an n-dimensional sphere is concentrated mainly on the surface of the sphere as the dimension becomes large. It is also known that, if we intersect a lattice with a n-dimensional sphere, then most of the lattice points will be concentrated very close to the surface [50]. In the course of our proof, we will show that the sum of any two such randomly chosen lattice points is also concentrated on a thin spherical shell $T^{\Delta}_{\sqrt{2P}}$ at a radius of $\sqrt{2nP}$ (see Fig. 18). Hence, the probability of error will be largely dependent on the lattice points in the thin spherical shell $T^{\Delta}_{\sqrt{2P}}$. We will use Blichfeldt's principle to show that, there exists translations (one for each user) of the lattice Λ_n, such that the sums of pairs of lattice points are concentrated in a thin spherical shell(see theorem J.1, lemma J.3 and lemma J.4). We next perform minimum angle decoding. In minimum angle decoding, we are interested only in the angle between the different lattice points on the thin spherical shell. It must be noted that the choice of the lattice Λ_n must be such that it acts as a good channel code. Minkowski-Hlawka theorem (theorem J.2 and lemma J.5) can be used to show existence of such lattices. Choosing the volume of the lattice's Voronoi region appropriately allows us to compute the achievable rate of this scheme.

3. Detailed proof for MAC phase

First we provide some definitions and notation.

- Λ_n denotes an n-dimensional lattice and let $\mathcal{V}_n$ be the basic Voronoi region of the lattice.
- $\mathbf{s}_1, \mathbf{s}_2$ are two n-dimensional translational vectors and $\mathbf{s}_1, \mathbf{s}_2 \in \mathcal{V}_n$.
- $\mathcal{L}(\mathbf{s}, T)$ is defined as the set of lattice points translated by a vector $\mathbf{s}$ present in the region T, i.e., $\mathcal{L}(\mathbf{s}, T) \triangleq (\Lambda_n + \mathbf{s}) \cap T$.
- $T_{\sqrt{P}}$ and $T_{\sqrt{2P}}$ represents n-dimensional hyperspheres centered at the origin with

radius of $\sqrt{nP}$ and $\sqrt{n2P}$, respectively.

- $T^{\Delta}_{\sqrt{2P}}$ represents an n-dimensional thin spherical shell around the radius $\sqrt{n2P}$ and is defined as $T^{\Delta}_{\sqrt{2P}} \triangleq \{\mathbf{x} \in \mathbb{R}^n : \sqrt{n(2P-\delta)} \leq \|\mathbf{x}\| \leq \sqrt{n(2P+\delta)}\}$, $\delta > 0$.

- $T'_{\sqrt{2P}}$ represents the region that does not contain the thin spherical shell and is defined as $T'_{\sqrt{2P}} \triangleq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq \sqrt{n(2P-\delta)}$ or $\|\mathbf{x}\| \geq \sqrt{n(2P+\delta)}\}$, $\delta > 0$.

- $\mathcal{C}_1$ and $\mathcal{C}_2$ are codebooks formed by the intersection of translations of the lattice Λ_n with hyperspheres, and are given by, $\mathcal{C}_1 \triangleq \mathcal{L}(\mathbf{s}_1, T_{\sqrt{P}}) = (\Lambda_n + \mathbf{s}_1) \cap T_{\sqrt{P}}$ and $\mathcal{C}_2 \triangleq \mathcal{L}(\mathbf{s}_2, T_{\sqrt{P}}) = (\Lambda_n + \mathbf{s}_2) \cap T_{\sqrt{P}}$.

- Similarly $\mathcal{C}_{\sqrt{2P}}$ is given as $\mathcal{C}_{\sqrt{2P}} \triangleq \mathcal{L}(\mathbf{s}_1 + \mathbf{s}_2, T_{\sqrt{2P}}) = (\Lambda_n + \mathbf{s}_1 + \mathbf{s}_2) \cap T_{\sqrt{2P}}$ and $\mathcal{C}^{\Delta}_{\sqrt{2P}}$ is given by $\mathcal{C}^{\Delta}_{\sqrt{2P}} \triangleq \mathcal{L}(\mathbf{s}_1 + \mathbf{s}_2, T^{\Delta}_{\sqrt{2P}}) = (\Lambda_n + \mathbf{s}_1 + \mathbf{s}_2) \cap T^{\Delta}_{\sqrt{2P}}$.

- Let $\mathcal{C}_{\oplus}$ be defined as $\mathcal{C}_{\oplus} \triangleq \mathcal{C}_1 \times \mathcal{C}_2 = \{(\mathbf{x}_1, \mathbf{x}_2) : \mathbf{x}_1 \in \mathcal{C}_1, \mathbf{x}_2 \in \mathcal{C}_2\}$. This denotes the combined collection of pairs of codewords of both the transmitters.

- Let $\mathcal{C}^{\Delta}_{\oplus} \triangleq \{(\mathbf{x}_1, \mathbf{x}_2) : \mathbf{x}_1 + \mathbf{x}_2 \in T^{\Delta}_{\sqrt{2P}}, \mathbf{x}_1 \in \mathcal{C}_1, \mathbf{x}_2 \in \mathcal{C}_2\}$. This denotes the codeword pairs whose sum lies on the thin shell $T^{\Delta}_{\sqrt{2P}}$.

- Let $\mathcal{C}'_{\oplus} \triangleq \mathcal{C}_{\oplus} \setminus \mathcal{C}^{\Delta}_{\oplus}$. This denotes the code word pairs whose sum does not lie on the thin shell. It must be noted that the set formed by the sum of codewords in $\mathcal{C}^{\Delta}_{\oplus}$ need not be the same as $\mathcal{C}^{\Delta}_{\sqrt{2P}}$ and at low SNRs, this may lead to a significant difference between ML and minimum angle decoding in the achievable exchange rate.

- Let $M_1(\Lambda_n, \mathbf{s}_1)$, $M_2(\Lambda_n, \mathbf{s}_2)$, $M_{\oplus}(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2)$, $M^{\Delta}_{\oplus}(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2)$ and $M'_{\oplus}(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2)$ denote the cardinality of $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_{\oplus}$, $\mathcal{C}^{\Delta}_{\oplus}$ and $\mathcal{C}'_{\oplus}$, respectively.

- For a given code $\mathcal{C}$, let us denote the average probability of error, under minimum distance decoding as $\mathcal{P}_e^{\mathcal{C}}$.
- Let us define a projection function π. This projects a n dimensional vector onto to an inner sphere of radius $\sqrt{n(2P-\delta)}$. It is defined as $\pi(\mathbf{x}) = (\sqrt{n(2P-\delta)}/\|\mathbf{x}\|)\mathbf{x}$.
- We also define an indicator function $\chi_T(\mathbf{x})$ as $\chi_T(\mathbf{x}) = 1,$ if $\mathbf{x} \in T$ and $\chi_T(\mathbf{x}) = 0,$ if $\mathbf{x} \notin T$.

We first start with the average probability of error for the minimum distance decoder and progressively show that it can be bounded by the average probability of error of a minimum angle decoder. It is easy to see that minimum distance decoding is equivalent to maximum likelihood decoding in the presence of Gaussian noise. As mentioned before, the set of pairs of lattice points whose sum lies in the thin spherical shell $T^{\Delta}_{\sqrt{2P}}$ is much larger than the pairs of lattice points whose sum lies outside the spherical region. Hence the average probability of error will not be affected much by these lattice points. This motivates us to express the average probability of error $\mathcal{P}_e^{\mathcal{C}_\oplus}$ as a sum of two terms. Notice that the decoding error is due to the relay decoding to a lattice point $\mathbf{x}'_{sum}$, where $\mathbf{x}_1, \mathbf{x}_2$ are the transmitted lattice vectors and $\mathbf{x}'_{sum} \neq (\mathbf{x}_1 + \mathbf{x}_2)$. This is made more clear in the lemma given below.

Lemma G.1.

$$\mathcal{P}_e^{\mathcal{C}_\oplus} \leq \frac{M'_\oplus}{M_\oplus} + \frac{1}{M_\oplus} \sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{C}^{\Delta}_{\oplus}} \Pr[\mathcal{E}(\mathbf{x}_1,\mathbf{x}_2)],$$

where $\mathcal{E}(\mathbf{x}_1,\mathbf{x}_2)$ is the event that $\pi(\mathbf{x}_1+\mathbf{x}_2)+Z^n$ is closest in Euclidean distance to $\pi(\mathbf{x}'_1+\mathbf{x}'_2)$, with $\mathbf{x}_1+\mathbf{x}_2 \neq \mathbf{x}'_1+\mathbf{x}'_2$ and $(\mathbf{x}'_1,\mathbf{x}'_2) \in C^{\Delta}_{\oplus}$.

Proof. Let the ordered pair $(\mathbf{x_1}, \mathbf{x_2}) \in \mathcal{C}_{\oplus}$, denote that $\mathbf{x_1} \in \mathcal{C}_1$ and $\mathbf{x_2} \in \mathcal{C}_2$. We next follow similar steps of the proof as given in [50].

$$\begin{aligned}
P_e^{\mathcal{C}_{\oplus}} &= \frac{1}{M_{\oplus}} \sum_{(\mathbf{x_1},\mathbf{x_2}) \in \mathcal{C}_{\oplus}} \Pr[\text{Error in decoding to } (\mathbf{x}_1 + \mathbf{x}_2)] \\
&\overset{(a)}{\leq} \frac{1}{M_{\oplus}} \sum_{(\mathbf{x_1},\mathbf{x_2}) \in \mathcal{C}'_{\oplus}} 1 + \frac{1}{M_{\oplus}} \sum_{(\mathbf{x_1},\mathbf{x_2}) \in \mathcal{C}^{\Delta}_{\oplus}} \Pr[\text{Error in decoding to } (\mathbf{x}_1 + \mathbf{x}_2)] \\
&= \frac{M'_{\oplus}}{M_{\oplus}} + \frac{1}{M_{\oplus}} \sum_{(\mathbf{x_1},\mathbf{x_2}) \in \mathcal{C}^{\Delta}_{\oplus}} \Pr[\text{Error in decoding to } (\mathbf{x}_1 + \mathbf{x}_2)] \\
&\overset{(b)}{\leq} \frac{M'_{\oplus}}{M_{\oplus}} + \frac{1}{M_{\oplus}} \sum_{(\mathbf{x_1},\mathbf{x_2}) \in \mathcal{C}^{\Delta}_{\oplus}} \Pr[\mathcal{E}(\mathbf{x}_1, \mathbf{x}_2)]
\end{aligned}$$

Here in (a) the first term follows by bounding the probability of error by 1, when $(\mathbf{x_1}, \mathbf{x_2}) \in \mathcal{C}'_{\oplus}$. In (b), $\mathcal{E}(\mathbf{x}_1, \mathbf{x}_2)$ captures the error event of the relay not decoding to $\pi(\mathbf{x}_1 + \mathbf{x}_2)$, where $\pi(\cdot)$ is the projection function that projects $(\mathbf{x}_1 + \mathbf{x}_2)$ to the inner sphere. This probability of this event, $\mathcal{E}(\mathbf{x}_1, \mathbf{x}_2)$ can be shown to be lesser than the probability of error in decoding to $(\mathbf{x}_1 + \mathbf{x}_2)$ by referring to the discussions on [50, Lemma 2].

$\square$

The first term on the right of the inequality in lemma G.1 follows by assuming that, we always make an error if the sum of the transmitted lattice points falls outside the thin spherical shell. The second term follows, since the probability of error increases, if decoding is performed based on the projection of lattice points on to the inner sphere. Since we are interested in lattice points projected on to the inner sphere of radius $\sqrt{n(2P - \delta)}$, we can define a decoding algorithm that looks at the angle between the lattice points, the minimum angle decoder. We next establish some more definitions. Let $B_{\theta}(\mathbf{y})$ denote an n-dimensional cone centered at the origin and having the axis passing through $\mathbf{y}$. Let θ be the half-angle of the cone and $\mathbf{y} \in \mathbb{R}^n$ be non-zero.

We next define a region related to our sub-optimum decoding function as follows,

$$A_\theta(\mathbf{x}_1, \mathbf{x}_2) = B_\theta(\mathbf{x}_1 + \mathbf{x}_2) \setminus \bigcup_{\mathbf{x}' \in \mathcal{C}^{\Delta}_{\sqrt{2P}} \setminus \{\mathbf{x}_1 + \mathbf{x}_2\}} B_\theta(\mathbf{x}')$$

or this can also be expressed as

$$A^C_\theta(\mathbf{x}_1, \mathbf{x}_2) = B^C_\theta(\mathbf{x}_1 + \mathbf{x}_2) \bigcup_{\mathbf{x}' \in \mathcal{C}^{\Delta}_{\sqrt{2P}} \setminus \{\mathbf{x}_1 + \mathbf{x}_2\}} B_\theta(\mathbf{x}').$$

$A_\theta(\mathbf{x}_1, \mathbf{x}_2)$ represents the region of the cone $B_\theta(\mathbf{x}_1 + \mathbf{x}_2)$, that does not intersect with any other cone corresponding to the other lattice codeword points $\mathbf{x}'$, located in the thin spherical shell. During decoding, when we receive a vector that falls in the region $A_\theta(\mathbf{x}_1, \mathbf{x}_2)$, we decode to the sum codeword $(\mathbf{x}_1 + \mathbf{x}_2)$. It may not be possible to decode to the individual codewords $\mathbf{x}_1$ and $\mathbf{x}_2$, as different pairs of codewords may yield the same sum. However it must be noted, that in the forward phase, we are interested in decoding only to the sum of the transmitted codewords.

Let $\mathcal{P}_\theta$ denote the probability of error using the sub-optimum decoder. Then, we have

$$\begin{aligned}
\mathcal{P}_\theta^{\pi(\mathcal{C}^{\Delta}_{\oplus})}(\mathbf{x}_1, \mathbf{x}_2) &\triangleq \Pr\left(\pi(\mathbf{x}_1 + \mathbf{x}_2) + Z^n \in A^C_\theta(\mathbf{x}_1, \mathbf{x}_2)\right) \\
&\overset{(a)}{\leq} \Pr\left(\pi(\mathbf{x}_1 + \mathbf{x}_2) + Z^n \notin B_\theta(\mathbf{x}_1 + \mathbf{x}_2)\right) \\
&\qquad + \sum_{\mathbf{x}' \in \mathcal{C}^{\Delta}_{\sqrt{2P}} \setminus \{\mathbf{x}_1 + \mathbf{x}_2\}} \Pr\left(\pi(\mathbf{x}_1 + \mathbf{x}_2) + Z^n \in B_\theta(\mathbf{x}')\right) \\
&\overset{(b)}{=} \Pr\left(\mathbf{t}_0 + Z^n \notin B_\theta(\mathbf{t}_0)\right) + \sum_{\mathbf{x}' \in \mathcal{C}^{\Delta}_{\sqrt{2P}} \setminus \{\mathbf{x}_1 + \mathbf{x}_2\}} p_\theta\left(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}'\right) \\
&\overset{(c)}{=} \Pr\left(\mathbf{t}_0 + Z^n \notin B_\theta(\mathbf{t}_0)\right)
\end{aligned}$$

$$+ \sum_{g \in \Lambda_n \setminus \{0\}} p_\theta\left(\mathbf{x}_1 + \mathbf{x}_2, g + \mathbf{x}_1 + \mathbf{x}_2\right) \chi_{T^{\Delta}_{\sqrt{2P}}}(g + \mathbf{x}_1 + \mathbf{x}_2)$$

First, $\Pr[\mathcal{E}(\mathbf{x}_1, \mathbf{x}_2)]$ can be clearly bounded from above by both the minimum angle decoder and the suboptimum decoder $\mathcal{P}_\theta^{\pi(\mathcal{C}_\oplus^\Delta)}(\mathbf{x}_1, \mathbf{x}_2)$. Next (a) follows because we use the union bound. In (b), the first term follows, because due to symmetry the probability is not dependent on the particular $\mathbf{x}_1 + \mathbf{x}_2$. The second term follows as we define $p_\theta(\mathbf{x}, \mathbf{x}')$ as $p_\theta(\mathbf{x}, \mathbf{x}') \triangleq \Pr(\pi(\mathbf{x}) + Z^n \notin B_\theta(\mathbf{x}'))$. In (c), we replace $\mathbf{x}'$, by $g + \mathbf{x}_1 + \mathbf{x}_2$ and the indicator function $\chi_{T^{\Delta}_{\sqrt{2P}}}$, corresponds to lattice points on the thin shell at radius $\sqrt{n2P}$.

Hence the average probability of error can be bounded as

$$\begin{aligned} \mathcal{P}_e^{\mathcal{C}_\oplus} \leq & \Pr\left(\mathbf{t}_0 + Z^n \notin B_\theta(\mathbf{t}_0)\right) + \frac{M'_\oplus}{M_\oplus} \\ & + \frac{1}{M_\oplus} \sum_{(\mathbf{x}_1, \mathbf{x}_2) \in \mathcal{C}_\oplus^\Delta} \sum_{g \in \Lambda_n \setminus \{0\}} p_\theta\left(\mathbf{x}_1 + \mathbf{x}_2, g + \mathbf{x}_1 + \mathbf{x}_2\right) \chi_{T^{\Delta}_{\sqrt{2P}}}(g + \mathbf{x}_1 + \mathbf{x}_2). \end{aligned} \tag{4.9}$$

The rest of the proof deals with bounding each of the three terms in the above equation by an arbitrarily small quantity, to make the probability of error tend to zero as $n \to \infty$. Below we briefly explain the requirements.

- The first term can be made very small by choosing the angle θ appropriately. In effect, we need the noise Z^n to be contained inside the cone $B_\theta(\mathbf{t}_0)$ with high probability as the dimension n becomes large.

- For the second term we need the number of codeword pairs whose sum of codewords lies outside the thin spherical shell to be shown to be much lesser than the total number of codeword pairs. In other words, we need to show that the sum of lattice points are concentrated in the thin spherical shell around the radius $\sqrt{n2P}$. This is shown in Lemma J.3.

- The third term has a summation which is difficult to evaluate and, hence, we bound it by an integral and evaluate the resulting integral.

- Finally, we require that the number of codewords in each of the inner spheres to be sufficiently large to achieve rates close to $\frac{1}{2}\log(\frac{1}{2}+SNR)$.

Blichfeldt's principle(see Theorem J.1) can be applied to show concentration of codeword pairs. Lemma J.4 in appendix J-C, is an application of Blichfeldt's principle that guarantees that for any given lattice, we can find translations that satisfy $\frac{M'_{\oplus}}{M_{\oplus}} \leq 4\frac{V'_{\oplus}}{V_{\oplus}}$, where $\frac{V'_{\oplus}}{V_{\oplus}}$ is a quantity that tends to 0 as the dimensions become large. Also it makes sure that we can find enough codewords in the hyperspheres of radius $\sqrt{nP}$, such that we can achieve a rate of $\frac{1}{2}\log(\frac{1}{2}+SNR)$.

Minkowski-Hlawka theorem (see Theorem J.2 in appendix J-A) is used to establish the existence of at least one lattice Λ_n^* such that the summation of the third term can be bounded by an integral. This theorem along with lemma J.4 in appendix J-C, are used together in lemma J.5 to obtain bounds on both the second and third term. Hence we can effectively rewrite (4.9) by using these bounds to get

$$\mathcal{P}_e^{\mathcal{C}_\oplus} \leq \Pr\left(\mathbf{t}_0 + Z^n \notin B_\theta(\mathbf{t}_0)\right) + 4\frac{V'_{\oplus}}{V_{\oplus}} + \left[\frac{2(n-1)\pi^{\frac{n-1}{2}}(n(2P+\delta))^{n/2}}{d_n n\Gamma(\frac{n+1}{2})}\int_0^\theta \sin^{n-2}(x)dx\right], \tag{4.10}$$

where d_n is the volume of the fundamental Voronoi region of the lattice Λ_n^*, and the terms $V_\oplus$ and $V'_\oplus$ are defined in (4.20) and (4.21), respectively. We can bound the integral, as shown in [53, p. 623–624] to get

$$\mathcal{P}_e^{\mathcal{C}_\oplus} \leq \Pr\left(\mathbf{t}_0 + Z^n \notin B_\theta(\mathbf{t}_0)\right) + 4\frac{V'_{\oplus}}{V_{\oplus}} + \left[\frac{2\pi^{\frac{n-1}{2}}(n(2P+\delta))^{n/2}}{d_n n\Gamma(\frac{n+1}{2})}\frac{\sin^{n-1}(\theta)}{\cos\theta}\right]. \tag{4.11}$$

We next need to choose the appropriate values for θ and d_n to make the probabilities tend to 0. For the first term, consider $\sin\angle(\mathbf{t}_0 + Z^n, \mathbf{t}_0)$ and note that

$$\sin\angle(\mathbf{t}_0 + Z^n, \mathbf{t}_0) = \sqrt{\frac{\|Z^n_\perp\|^2}{\left(\sqrt{n(2P-\delta)} + Z^n_\parallel\right)^2 + \|Z^n_\perp\|^2}} \overset{n\to\infty}{\longrightarrow} \sqrt{\frac{\sigma^2}{2P-\delta+\sigma^2}}$$

with probability 1, where $Z^n_\parallel$ is the projection of the random vector Z^n along the direction of $\mathbf{t}_0$ and $Z^n_\perp$ is the projection of the random vector Z^n on the null space of $\mathbf{t}_0$. Hence we choose $\sin\theta = \sqrt{\frac{\sigma^2}{2P-\delta+\sigma^2}}$. For the third term a good choice of d_n is

$$d_n = V_n(\sqrt{n(2P+2\delta)})\sin^n\theta = \frac{\pi^{n/2}(n(2P+2\delta))^{n/2}(\sin^n\theta)}{\Gamma(n/2+1)}, \tag{4.12}$$

where $V_n(r)$ is the volume of an $n-$dimensional sphere of radius r. This choice helps us to make the third term tend to 0 for large n. The third term then can be rewritten as given below. We use the results in [50, p. 277], to bound the Gamma functions to get,

$$\begin{aligned}\left[2\frac{\pi^{\frac{n-1}{2}}(n(2P+\delta))^{n/2}}{d_n n\Gamma(\frac{n+1}{2})}\frac{\sin^{n-1}(\theta)}{\cos\theta}\right] &= \frac{2}{\sqrt{\pi}\sin\theta\cos\theta}\left(\frac{2P+\delta}{2P+2\delta}\right)^{n/2}\frac{\Gamma(\frac{n}{2}+1)}{n\Gamma(\frac{n+1}{2})}\\ &< \frac{2}{\sqrt{\pi}\sin\theta\cos\theta}\left(\frac{2P+\delta}{2P+2\delta}\right)^{n/2}\frac{1}{2}\frac{\left[1+\Gamma(\frac{n+1}{2})\right]}{\Gamma(\frac{n+1}{2})}\end{aligned}$$

This decays to 0 exponentially as $n\to\infty$. Also, from lemma J.3 we can show that $\frac{V'_\oplus}{V_\oplus} \to 0$ as $n\to\infty$.

Now, the achievable rate can be obtained from the number of lattice points in the sphere of radius $\sqrt{nP}$. This value $M_1(\Lambda^*_n, \mathbf{s}^*_1)$, $M_2(\Lambda^*_n, \mathbf{s}^*_{\mathbf{2}})$ from lemma J.5, can be seen to be greater than $\frac{V_n(\sqrt{nP})}{8d_n}$. Hence the rate $R_{Lattice}$ is given by,

$$\begin{aligned}
R_{Lattice} &\geq \frac{1}{n}\log M_1(\Lambda_n^*, \mathbf{s}_1^*), \frac{1}{n}\log M_2(\Lambda_n^*, \mathbf{s}_2^*) \\
&\geq \frac{1}{n}\log \frac{V_n(\sqrt{nP})}{8d_n} \\
&\overset{(a)}{\geq} \frac{1}{n}\log\left[\frac{1}{8}\left(\frac{P}{(2P+2\delta)\sin^2\theta}\right)^{n/2}\right] \\
&\overset{(b)}{\geq} \frac{1}{2}\log\left(\frac{P}{2P+2\delta} + \left(\frac{2P-\delta}{2P+2\delta}\right)\frac{P}{\sigma^2}\right) - \frac{\log 8}{n} \\
&\geq \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right) - \delta'.
\end{aligned}$$

In the above inequalities, (a) follows by substituting for d_n from (4.12) and (b) follows by choosing $\sin\theta = \sqrt{\frac{\sigma^2}{2P-\delta+\sigma^2}}$. Choosing δ' arbitrarily small, a rate of $\frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\sigma^2}\right)$ can be exchanged.

4. Broadcast phase

In the broadcast phase, we cannot directly transmit the sum of lattice points to the nodes. This will violate the transmit power constraint at the relay. Hence we perform Slepian-Wolf coding at the broadcast phase which requires coding over long block lengths. This can be accomplished by dividing the transmission in the MAC phase into l blocks of m channel uses each such that $n = lm$. Nodes A and B will use lattices of dimension m (i.e., each codeword spans m channel uses) instead of n and transmits l such codewords in the MAC phase.

The relay performs minimum angle decoding over an m-dimensional lattice and the relay decodes to the lattice point $\mathbf{x}_R = (\mathbf{x}_1 + \mathbf{x}_2)$. Here, both $\mathbf{x}_1$ and $\mathbf{x}_2$ are m-dimensional vectors.

During the broadcast phase, we treat each $m-$dimensional lattice point as a symbol and perform Slepian-Wolf coding over l symbols at a rate R_{SW}. In Slepian-

Wolf coding, $\mathbf{x}_R$ is considered as the source to be encoded and the side information available at the nodes A and B is $\mathbf{x}_1$ and $\mathbf{x}_2$, respectively. However, notice that the correlation between $\mathbf{x}_R$ and $\mathbf{x}_1$ is statistically identical to the correlation between $\mathbf{x}_R$ and $\mathbf{x}_2$. Hence, we can perform Slepian-Wolf coding assuming either $\mathbf{x}_1$ or $\mathbf{x}_2$ is the side information available at the receiver. The index which represents Slepian-Wolf encoding is then broadcast to both nodes.

By making m and l both arbitrarily large as $n \to \infty$, the required rate R_{SW} is given by

$$\begin{aligned} R_{SW} &= \frac{1}{m} H(\mathbf{X}_R|\mathbf{X}_1) = \frac{1}{n} H(\mathbf{X}_2) = \frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right) \\ &= \frac{1}{m} H(\mathbf{X}_R|\mathbf{X}_2) = \frac{1}{n} H(\mathbf{X}_1) = \frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right) \end{aligned}$$

Since the capacity of the channel from the relay to the nodes is $\frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$, the Slepian-Wolf encoded index can be broadcast to the nodes, with an arbitrarily low probability of error. Hence, it is possible for the nodes A and B to decode their intended messages after decoding in the broadcast phase at a rate of $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right)$, which proves theorem G.1.

5. General remarks

There may two reasons for the suboptimality of the minimum angle decoder. Firstly, the set of codewords of the form $\{\mathbf{x}_1 + \mathbf{x}_2\}$ is the codebook induced at the relay through the addition of two lattice points. The codewords in this set of points do not occur with equal probability. The minimum angle decoder does not take in to account this unequal distribution of the codewords in the induced codebook. Secondly, at low SNRs, the set of points in $\mathcal{C}^{\Delta}_{\sqrt{2P}}$ may not all be points of the induced codebook for $\{\mathbf{x}_1 + \mathbf{x}_2\}$, i.e., the set $\mathcal{C}^{\Delta}_{\oplus}$ may not be the same as $\mathcal{C}^{\Delta}_{\sqrt{2P}}$. The analysis of the minimum angle decoder ignores this also. Hence we deduce that this may lead to sub-optimality at low SNRs and the MAP decoder may give a better performance at this SNR range.

Though the results of the minimum angle decoding discussed here are for the symmetric case, they can be easily extended for the asymmetric case by following similar steps as discussed in this section. In the asymmetric case the nodes have two different transmit power constraints namely P_1 and P_2, and we can obtain the same exchange rate results contained in the recent work [42] using the minimum angle decoder.

H. Joint decoding based scheme

While the aforementioned scheme is nearly optimal at high SNR, the performance of this scheme at low SNR is very poor. In fact, for $P/\sigma^2 < 1/2$, the scheme does not even provide a non-zero rate. In this regime, we can use any coding scheme which is optimal for the multiple access channel and perform joint decoding at the relay such that $\mathbf{u}_1$ and $\mathbf{u}_2$ can be decoded. Then, the relay can encode $\mathbf{u}_1 \oplus \mathbf{u}_2$ and transmit to the nodes. Any coding scheme that is optimal for the MAC channel can be used in the MAC phase. A simple scheme is time sharing (although it is not the only one) where nodes A and B transmit with powers $2P$ for a duration of $n/2$ channel uses each but they do not interfere with one another. In this case, a rate of

$$R_{JD} = \frac{1}{4} \log \left(1 + \frac{2P}{\sigma^2} \right) \tag{4.13}$$

can be obtained. It can be seen that this is optimal at asymptotically low SNR, since $\log(1 + \mathsf{snr}) \approx \mathsf{snr}$ for $\mathsf{snr} \to 0$.

The performance of these schemes is shown in Fig. 19 where the upper bound

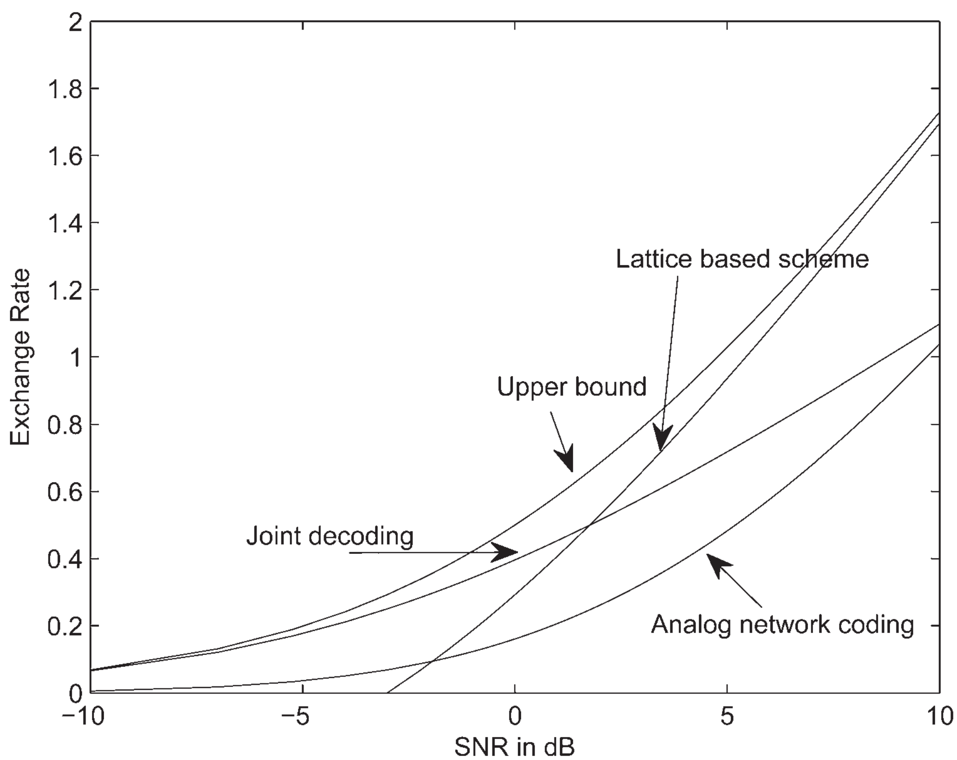

Fig. 19. Achievable exchange rates for the proposed schemes.

and the achievable rates with these proposed schemes are compared. The achievable rate with the analog network coding scheme is also shown. It can be seen that our schemes outperform analog network coding. However, it must be noted here that the scheme proposed here requires perfect synchronization of the phases from the transmissions, whereas the analog network coding scheme does not.

Clearly, we can time share between the lattice based scheme and the joint decoding based scheme in order to obtain rates of the form

$$R_{ex} = \beta R_{ex,JD} + (1-\beta) R_{Lattice}. \tag{4.14}$$

It can be shown that between the SNRs of -0.659 dB and 3.46 dB, time sharing between the two schemes results in better rates than the individual schemes. In both the lattice based scheme and the joint decoding based scheme, if the restriction to use n channel uses during the MAC phase and n during the broadcast phase is removed, i.e., only the total number of uses is constrained to be $2n$, better schemes can be easily designed. Similarly, different power sharing may also lead to better schemes.

I. Conclusion

We considered joint physical layer and network layer coding for the bi-directional relay problem where two nodes wish to exchange information through AWGN channels. Under the restrictive model of the MAC and broadcast phase using n channel uses separately, we showed upper bounds on the exchange capacity and constructive schemes based on lattices that are nearly optimal at high SNR. At low SNR joint decoding based schemes (optimal coding schemes for the MAC channel) are nearly optimal. These schemes outperform the recently proposed analog network coding schemes. Interestingly, our result shows that structured codes such as lattice codes outperform random codes for such networking problems. We also showed that minimum angle decoding also leads to similar results. An interesting future work is to obtain better exchange rates at low SNRs using structured lattice codes.

J. Appendix

1. Nested lattice encoding/decoding proof

In this section we state without proof lemma J.1 and J.2 mentioned in the proof of theorem F.1. We first restate some of the definitions in [46]. Let $\mathcal{R}_u$ be the covering radius of Λ_c and let $\mathcal{B}(\mathcal{R}_u)$ be the n-dimensional ball of radius $\mathcal{R}_u$. Let ρ^2 be the second moment (per dimension) of the smallest ball containing $\mathcal{V}(\Lambda_c)$, i.e.,

$$\rho^2 = \frac{1}{n}\frac{1}{\|\mathcal{B}(\mathcal{R}_u)\|}\int_{\mathcal{B}(\mathcal{R}_u)} \|\mathbf{u}\|^2 d\mathbf{u}. \tag{4.15}$$

Note that $\mathcal{V}(\Lambda_c)$ has a second moment P and hence $P < \rho^2$. Let $\mathbf{Z}^*$ be a random variable given by $\mathbf{Z}^* = (1-\alpha)(\mathbf{Z}_1+\mathbf{Z}_2)+\alpha\mathbf{Z}$, with $\mathbf{Z}_1 \sim \mathcal{N}(0, \rho^2\mathbf{I}^n)$, $\mathbf{Z}_2 \sim \mathcal{N}(0, \rho^2\mathbf{I}^n)$ and $\mathbf{Z} \sim \mathcal{N}(0, \sigma^2\mathbf{I}^n)$, where $\mathbf{I}^n$ is the $n \times n$ identity matrix. Then, the variance of $\mathbf{Z}^*$ satisfies the bounds expressed in the following lemma.

Lemma J.1 (Modified version of [46, Lemma 6])**.** *For a given lattice Λ_c, let $\mathcal{R}_u$ be the covering radius and let $\mathcal{R}_l$ be the radius of the n-dimensional hypersphere whose volume is equal to the volume of the basic Voronoi region $\mathcal{V}(\Lambda_c)$. Also let ρ^2 be defined as in (4.15) and let $\alpha = \frac{2P}{2P+\sigma^2}$, then the variance of $\mathbf{Z}^*$ per unit dimension,* $\mathrm{Var}(\mathbf{Z}^*)$ *depends on the parameters of the lattice Λ_c as follows,*

$$\frac{n}{n+2}.\frac{2P\sigma^2}{2P+\sigma^2} \leq \mathrm{Var}(\mathbf{Z}^*) = (1-\alpha)^2(\rho^2+\rho^2)+\alpha^2\sigma^2 < \left(\frac{R_u}{R_l}\right)^2 \frac{2P\sigma^2}{2P+\sigma^2}. \tag{4.16}$$

Proof. The proof of the above lemma closely follows the proof in [46]. Equations [46, 116-118] can be used to get a bound on $\mathrm{Var}(Z_1)$ and $\mathrm{Var}(Z_2)$, i.e., ρ^2. Choosing $\alpha = \frac{2P}{2P+\sigma^2}$, the modified version of [46, Lemma 6] can be proved. $\square$

Let $\mathbf{X}_1$ and $\mathbf{X}_2$ be two independent random variables which are uniformly distributed over $\mathcal{V}(\Lambda_c)$ and let $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$ be an n-dimensional Gaussian vector independent of $\mathbf{X}_1$ and $\mathbf{X}_2$. Further, let $\mathbf{Z}_{eq} = (1-\alpha)(\mathbf{X}_1 + \mathbf{X}_2) + \alpha\mathbf{Z}$, where $\alpha = \frac{2P}{2P+\sigma^2}$. Notice that $\mathbf{Z}_{eq}$ is not Gaussian. We next state a lemma which is a modified version of [46, Lemma 11] by Erez and Zamir which essentially shows that there exists good lattices for which $\mathbf{Z}_{eq}$ can be well approximated by a Gaussian of nearly the same variance and the approximation gets better as $n \to \infty$.

Lemma J.2 (Modified version of [46, Lemma 11])**.** *Let Λ_c be a lattice which is both Rogers-good as well as Poltyrev-good [46, eqn. 78 of pg. 2306]. Then, for any $\mathbf{x}$,*

$$f_{\mathbf{Z}_{eq}}(\mathbf{x}) < e^{\epsilon_1(\Lambda_c)n} f_{\mathbf{Z}^*}(\mathbf{x}), \tag{4.17}$$

where $\epsilon_1(\Lambda_c) \to 0$ as $n \to \infty$.

Proof. To prove the modified version of [46, Lemma 11], we can repeat the steps in [46], and equation [46, 200] can be restated with the notation in this paper as

$$\frac{1}{n} \log \frac{f_{\mathbf{X_1}}(\mathbf{x})}{f_{\mathbf{Z_1}}(\mathbf{x})} = \epsilon_1(\Lambda_c) = \mathcal{O}\left(\frac{1}{n}\right). \tag{4.18}$$

Similarly for $\mathbf{Z}_2$, we get

$$\frac{1}{n} \log \frac{f_{\mathbf{X_2}}(\mathbf{x})}{f_{\mathbf{Z_2}}(\mathbf{x})} = \epsilon_1(\Lambda_c) = \mathcal{O}\left(\frac{1}{n}\right). \tag{4.19}$$

Combining (4.18) and (4.19) and also the definition of $\mathbf{Z}^*$ as $\mathbf{Z}^* = (1-\alpha)(\mathbf{Z_1} + \mathbf{Z_2}) + \alpha\mathbf{N}$, we can get the proof of the modified version of [46, Lemma 11]. $\square$

2. Blichfeldt's principle and Minkowski-Hlawka theorem

Theorem J.1 (Blichfeldt's principle [54]). *Let f be a Riemann integrable function with bounded support. If Λ_n is a lattice with fundamental region $\mathcal{V}_n$ then*

$$\int_{\mathbb{R}^n} f(\mathbf{s})dV(\mathbf{s}) = \int_{\mathcal{V}_n} \left(\sum_{h \in \Lambda_n} f(h+\mathbf{s}) \right) dV(\mathbf{s}).$$

Theorem J.2 (Minkowski-Hlawka [50, 54]). *Let f be a nonnegative Riemann integrable function with bounded support. Then for every $d \in \mathbb{R}^+$ and $n \geq 2$, there exists a lattice Λ_n with determinant $det(\Lambda_n) = d$ such that*

$$d \sum_{g \in \Lambda_n \setminus \{0\}} f(g) \leq \int f dV(\mathbf{x}).$$

Minkowski-Hlawka theorem gives us a way to connect a series of discrete sums with a continuous integral. This will find applications in our probability of error calculations.

We next define the quantities $V_\oplus$ and $V'_\oplus$ which will be useful in the proof for our minimum angle decoding scheme. $V_\oplus$ is defined as,

$$V_\oplus = \int \int \chi_{T_{\sqrt{P}}}(\mathbf{u}) \chi_{T_{\sqrt{P}}}(\mathbf{v}) dV(\mathbf{u}) dV(\mathbf{v}). \tag{4.20}$$

Here $V_\oplus = (V_n(\sqrt{nP}))^2$, represents the square of the volume of an n-dimensional sphere of radius $\sqrt{nP}$. dV represents the n-dimensional volume element in rectangular co-ordinates. Also, $V'_\oplus$ is defined as

$$V'_\oplus = \int \int \chi_{T_{\sqrt{P}}}(\mathbf{u}) \chi_{T_{\sqrt{P}}}(\mathbf{v}) \chi_{T'_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v}) dV(\mathbf{u}) dV(\mathbf{v}). \tag{4.21}$$

We next state without proof the following corollary which is an application of Blichfeldt's principle.

Corollary J.1. *For a given $n-$dimensional lattice Λ_n, we have*

$$V_{\oplus} = \int_{\mathcal{V}_n}\int_{\mathcal{V}_n} M_{\oplus}(\Lambda_n, \mathbf{s_1}, \mathbf{s_2}) dV(\mathbf{s_1}) dV(\mathbf{s_2})$$

$$\text{and } V'_{\oplus} = \int_{\mathcal{V}_n}\int_{\mathcal{V}_n} M'_{\oplus}(\Lambda_n, \mathbf{s_1}, \mathbf{s_2}) dV(\mathbf{s_1}) dV(\mathbf{s_2}).$$

Proof. Let us define a function

$$f(\mathbf{u}, \mathbf{v}) = \chi_T(\mathbf{u})\chi_T(\mathbf{v}). \tag{4.22}$$

For a fixed $\mathbf{u}$, $f(\mathbf{u}, \mathbf{v})$ can be seen as a function with bounded support and also can be seen to be integrable. Hence we can apply the Blichfeldt's principle to get

$$h(\mathbf{u}) = \int f(\mathbf{u}, \mathbf{v}) dV(\mathbf{v}) = \int_{\mathcal{V}_n} \left(\sum_{h_2 \in \Lambda_n} f(\mathbf{u}, h_2 + \mathbf{s_2}) \right) dV(\mathbf{s_2}).$$

Now $h(\mathbf{u})$ can again be seen as an integrable function with bounded support, and hence the Blichfeldt's principle could be applied again to get the following,

$$\begin{aligned}
V_{\oplus} &= \int h(\mathbf{u}) dV(\mathbf{u}) \\
&= \int_{\mathcal{V}_n} \sum_{h_1 \in \Lambda_n} \left(\int_{P_n} \left(\sum_{h_2 \in \Lambda_n} f(h_1 + \mathbf{s_1}, h_2 + \mathbf{s_2}) \right) dV(\mathbf{s_2}) \right) dV(\mathbf{s_1}) \\
&\overset{(a)}{=} \int_{\mathcal{V}_n}\int_{\mathcal{V}_n} \left(\sum_{h_1 \in \Lambda_n} \sum_{h_2 \in \Lambda_n} f(h_1 + \mathbf{s_1}, h_2 + \mathbf{s_2}) \right) dV(\mathbf{s_1}) dV(\mathbf{s_2}) \\
&\overset{(b)}{=} \int_{\mathcal{V}_n}\int_{\mathcal{V}_n} M_{\oplus}(\Lambda_n, \mathbf{s_1}, \mathbf{s_2}) dV(\mathbf{s_1}) dV(\mathbf{s_2})
\end{aligned}$$

Above (a) follows since we have a finite number of non-zero terms, and hence the integral and the summation can be interchanged. Also in (b), $M_{\oplus}(\Lambda_n, \mathbf{s_1}, \mathbf{s_2})$ is the number of pairs of lattice points for the translations $\mathbf{s_1}$ and $\mathbf{s_2}$. A similar approach can be used to obtain the expression for $V'_{\oplus}$. □

In short, corollary J.1 relates the square of the volume of an n-dimensional sphere

$V_{\oplus}$ and the number of pairs of lattice points $M_{\oplus}$ for different translations. Also, it relates $V'_{\oplus}$ and the number of pairs of lattice points $M'_{\oplus}$, whose sum falls outside a thin spherical shell at a radius of $\sqrt{2nP}$ from the origin. We next state a lemma which shows that the ratio $V'_{\oplus}/V_{\oplus}$ can be made arbitrarily small when the dimension n becomes large.

3. Hyper volume concentration lemma

Lemma J.3. *For every given $\delta > 0$, we can find an N_0 sufficiently large such that for all $n > N_0$, the ratio $\frac{V'_{\oplus}}{V_{\oplus}} < \delta$.*

The above lemma can also be interpreted as, that the vector sum of two points chosen uniformly over an $n-$dimensional sphere, concentrates with high probability over a thin shell.

Proof. First we perform a change of variables in the integral, by substituting $\mathbf{x} = \mathbf{u} + \mathbf{v}$. This gives from equation 4.21,

$$V'_{\oplus} = \int\int \chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{x}-\mathbf{u})\chi_{T'_{\sqrt{2P}}}(\mathbf{x})dV(\mathbf{u})dV(\mathbf{x}).$$

Let us consider first the inner integral, for a fixed $\mathbf{x}$,given by,

$$\int \chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{x}-\mathbf{u})dV(\mathbf{u}).$$

This geometrically represents the hypervolume of intersection of two hyperspheres, whose centers are at a distance $\|\mathbf{x}\|$, from each other. This is pictorially shown in Fig. 20. The calculation of hypervolume of intersection, reduces to obtaining the hypervolume of the conical section and a cone. This is shown pictorially in the second diagram in Fig. 20. Here *opq* represents the hyper cone and *oprq* represents

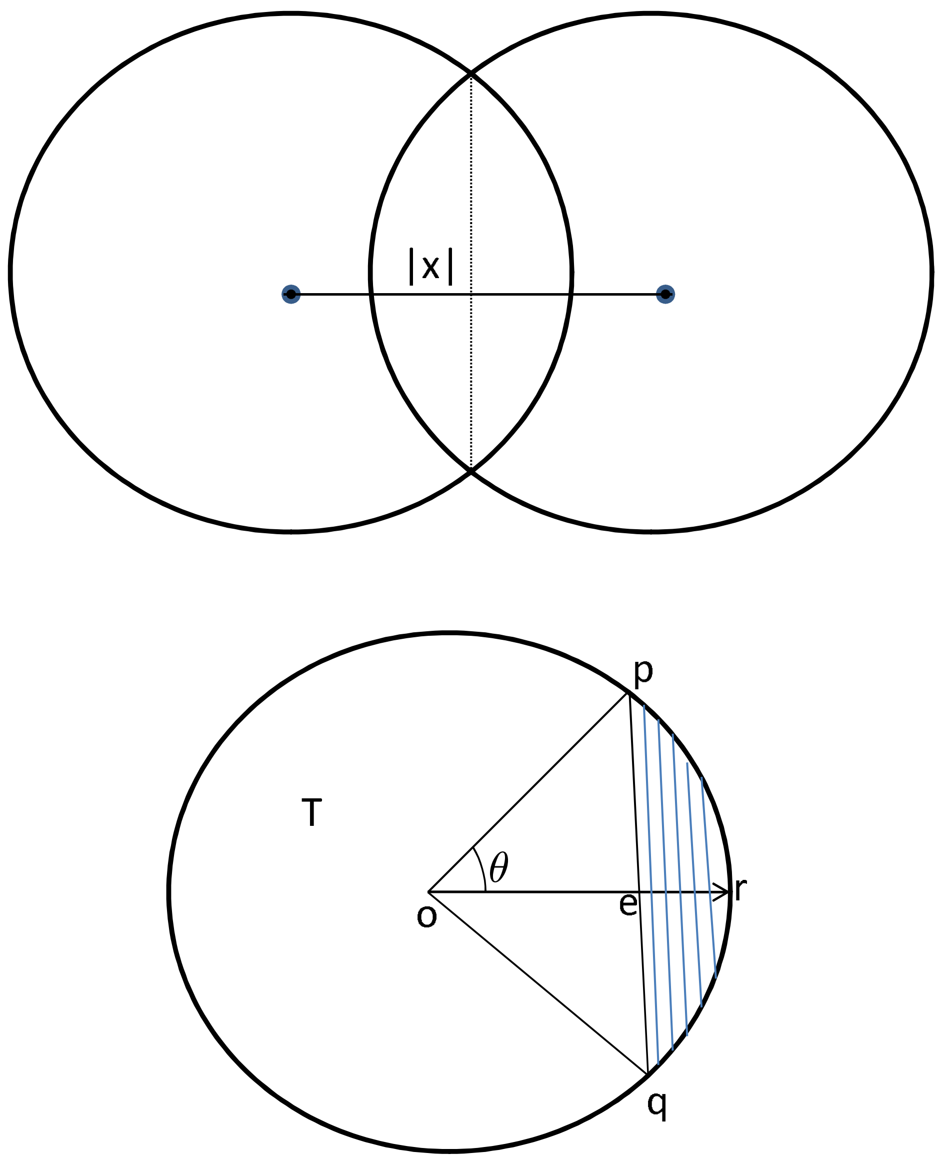

Fig. 20. Geometrical interpretation of the integral.

the conical section. Here we denote by $V_{cs}(|\mathbf{x}|)$ to represent the volume of the conical section and $V_{co}(|\mathbf{x}|)$ as the volume of the cone. The integral can hence be evaluated as

$$\int \chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{x}-\mathbf{u})dV(\mathbf{u}) = 2(V_{cs}(|\mathbf{x}|) - V_{co}(|\mathbf{x}|)).$$

To simplify calculations we can bound the integral as,

$$\int \chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{x}-\mathbf{u})dV(\mathbf{u}) \leq 2V_{cs}(|\mathbf{x}|).$$

From the figure we can see $oe = \|x\|/2$. Hence the half-angle θ can be calculated as $\cos\theta = \frac{oe}{\sqrt{nP}} = \frac{\|x\|}{2\sqrt{nP}}$. Hence with the defined θ, we can calculate the hypervolume as,

$$V_{cs}(|\mathbf{x}|) = 2\left(\int_{\psi=0}^{\theta} \sin^{n-2}\psi d\psi\right) \frac{\pi^{\frac{n-1}{2}}(nP)^{\frac{n}{2}}}{n\Gamma(\frac{n-1}{2})} \tag{4.23}$$

Hence,

$$\frac{V'_{\oplus}}{V_{\oplus}} \leq 2\int \frac{V_{cs}(\|\mathbf{x}\|)}{V_{\oplus}} \chi_{T'_{\sqrt{2P}}}(\mathbf{x})dV(\mathbf{x}) \tag{4.24}$$

But $V_{\oplus}$ is given by V^2, where V is the hypervolume of an n-dimensional hypersphere of radius $\sqrt{nP}$ denoted by $V_n(\sqrt{nP})$.

The value of $V_{cs}(\|x\|)$ depends only on the distance of $\mathbf{x}$ from the origin. To make evaluation of the integral easier, we change the volume element to circular co-ordinates and integrate. Thus the integral now becomes,

$$\frac{V'_{\oplus}}{V_{\oplus}} \leq 2\left(\frac{n\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\right) \int_{r\in l'_{\oplus}} \frac{V_{cs}(r)}{V_n(\sqrt{nP})^2}\, r^{n-1}dr, \tag{4.25}$$

where $l'_{\oplus}$ is defined as the union of closed intervals given by

$$l'_{\oplus} = \left[0, \sqrt{n(2P-\delta')}\right] \bigcup \left[\sqrt{n(2P+\delta')}, 2\sqrt{nP}\right]$$

and δ' is a small positive real number. Now substituting $V_{cs}(r)$ from above gives,

$$\frac{V'_\oplus}{V_\oplus} \leq 4\frac{n\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\frac{\pi^{\frac{n-1}{2}}(nP)^{\frac{n}{2}}}{n\Gamma(\frac{n-1}{2})}\int_{r\in l'_\oplus}\int_{\psi=0}^{\cos^{-1}(\frac{r}{2\sqrt{nP}})}\frac{r^{n-1}\sin^{n-2}\psi}{V_n(\sqrt{nP})^2}d\psi dr \tag{4.26}$$

Now let us choose $\cos\theta = \frac{r}{2\sqrt{nP}}$ and perform change of variables, defining ${\theta_\oplus}'$ as ${\theta_\oplus}' = \left\{\cos^{-1}\left(\frac{r}{2\sqrt{nP}}\right) : r \in {l_\oplus}'\right\}$.

$$\frac{V'_\oplus}{V_\oplus} \leq 4\frac{n\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\frac{\pi^{\frac{n-1}{2}}(nP)^{\frac{n}{2}}}{n\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus}(nP)^{n/2}\cos^{n-1}\theta\sin\theta\int_{\psi=0}^{\theta}\frac{2^n\sin^{n-2}\psi}{V_n(\sqrt{nP})^2}d\psi d\theta \tag{4.27}$$

Note that ${\theta_\oplus}'$ does not contain $\frac{\pi}{4}$. Substituting for $V_n(\sqrt{nP})$, we get,

$$\frac{V'_\oplus}{V_\oplus} \leq \frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus}2^n\cos^{n-1}\theta\sin\theta\int_{\psi=0}^{\theta}\sin^{n-2}\psi d\psi d\theta \tag{4.28}$$

$$\begin{aligned}\frac{V'_\oplus}{V_\oplus} \leq&\frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus\cap[0,\frac{\pi}{3}+\eta]}2^n\cos^{n-1}\theta\sin\theta\int_{\psi=0}^{\theta}\sin^{n-2}\psi d\psi d\theta\\&+\frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus\cap[\frac{\pi}{3}+\eta,\frac{\pi}{2}]}2^n\cos^{n-1}\theta\sin\theta\int_{\psi=0}^{\theta}\sin^{n-2}\psi d\psi d\theta,\end{aligned} \tag{4.29}$$

where η is a small positive real number. Now we will use the bound used in [53] for the first term. We can apply the bound for $\theta < \pi/2$. Hence we split the integral into two terms to apply the bound. For the second term we will bound $\sin\psi$ by 1. This gives,

$$\begin{aligned}\frac{V'_\oplus}{V_\oplus} \leq&\frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus\cap[0,\frac{\pi}{3}+\eta]}2^n\cos^{n-1}\theta\sin\theta\frac{\sin^{n-1}\theta}{(n-1)\cos\theta}d\theta\\&+\frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n-1}{2})}\int_{\theta\in\theta'_\oplus\cap[\frac{\pi}{3}+\eta,\frac{\pi}{2}]}2^n\cos^{n-1}\theta\sin\theta\int_{\psi=0}^{\theta}d\psi d\theta\end{aligned} \tag{4.30}$$

Simplifying things further we get,

$$\begin{aligned}\frac{V'_\oplus}{V_\oplus} \leq&\frac{4}{\sqrt{\pi}}\frac{\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n+1}{2})}\int_{\theta\in\theta'_\oplus\cap[0,\frac{\pi}{3}+\eta]}2^{n-1}\sin^{n-1}\theta\cos^{n-1}\theta\tan\theta d\theta\\&+\frac{4}{\sqrt{\pi}}\frac{(n-1)\Gamma(\frac{n}{2}+1)}{\Gamma(\frac{n+1}{2})}\int_{\theta\in\theta'_\oplus\cap[\frac{\pi}{3}+\eta,\frac{\pi}{2}]}2^{n-1}\cos^{n-1}\theta\sin\theta\frac{\pi}{2}d\theta\end{aligned} \tag{4.31}$$

Next we bound $\tan\theta$ in the first term by $\tan(\pi/3+\eta)$ and $\sin\theta$ in the second term by 1. We also bound the factorial using the bound given in [50]. This yields,

$$\begin{aligned}\frac{V'_{\oplus}}{V_{\oplus}} \leq \frac{4}{\sqrt{\pi}}\frac{\frac{n}{2}(1+\Gamma(\frac{n+1}{2}))\tan(\frac{\pi}{3}+\eta)}{\Gamma(\frac{n+1}{2})}\int_{\theta\in\theta'_{\oplus}\cap[0,\frac{\pi}{3}+\eta]}(\sin 2\theta)^{n-1}d\theta \\ +\frac{4}{\sqrt{\pi}}\frac{(n-1)\frac{n}{2}(1+\Gamma(\frac{n+1}{2}))}{\Gamma(\frac{n+1}{2})}\int_{\theta\in\theta'_{\oplus}\cap[\frac{\pi}{3}+\eta,\frac{\pi}{2}]}\frac{\pi}{2}(2\cos\theta)^{n-1}d\theta\end{aligned} \tag{4.32}$$

Again we can see that since θ does not take the value $\pi/4$ we can bound the first term appropriately. In the second term the maximum value of $\cos\theta$ can be used to bounded it appropriately. This is given below as follows.

$$\begin{aligned}\frac{V'_{\oplus}}{V_{\oplus}} \leq \frac{4}{\sqrt{\pi}}\frac{\frac{n}{2}(1+\Gamma(\frac{n+1}{2}))\tan(\frac{\pi}{3}+\eta)}{\Gamma(\frac{n+1}{2})}(\sin(\frac{\pi}{2}-2\epsilon))^{n-1}\frac{\pi}{2} \\ +\frac{4}{\sqrt{\pi}}\frac{(n-1)\frac{n}{2}(1+\Gamma(\frac{n+1}{2}))}{\Gamma(\frac{n+1}{2})}\frac{\pi}{2}[2\cos(\frac{\pi}{3}+\eta)]^{n-1}\frac{\pi}{2}\end{aligned} \tag{4.33}$$

From the above we can easily see, that both terms tend to 0 as $n\to\infty$. From this the lemma follows. □

4. Application of Blichfeldt's principle to show existence of good translations

Lemma J.4. *Let Λ_n be a lattice having a fundamental region $\mathcal{V}_n$ and let $det(\Lambda_n)$ be it's fundamental volume and define*

$$\mathcal{V}_n^* = \left\{(\mathbf{s}_1,\mathbf{s}_2)\in\mathcal{V}_n\times\mathcal{V}_n : M_1(\Lambda_n,\mathbf{s}_1)\geq\frac{V_n(\sqrt{nP})}{8det(\Lambda_n)}; M_2(\Lambda_n,\mathbf{s}_2)\geq\frac{V_n(\sqrt{nP})}{8det(\Lambda_n)};\right. \\ \left.\frac{M'_{\oplus}(\Lambda_n,\mathbf{s}_1,\mathbf{s}_2)}{M_{\oplus}(\Lambda_n,\mathbf{s}_1,\mathbf{s}_2)}\leq 4\frac{V'_{\oplus}}{V_{\oplus}}\right\}$$

Then $V_{\oplus}\leq 2\int_{\mathcal{V}_n^*}M_{\oplus}(\Lambda_n,\mathbf{s}_1,\mathbf{s}_2)dV(\mathbf{s}_1,\mathbf{s}_2)$. This implies that the measure of $\mathcal{V}_n^*$ must be non-zero and, hence, there must be at least some good translations $(\mathbf{s}_1^*,\mathbf{s}_2^*)$ of the lattice, such that $M_1(\Lambda_n,\mathbf{s}_1^*)\geq\frac{V_n(\sqrt{nP})}{8det(\Lambda_n)}$, $M_2(\Lambda_n,\mathbf{s}_2^*)\geq\frac{V_n(\sqrt{nP})}{8det(\Lambda_n)}$ and $\frac{M'_{\oplus}(\Lambda_n,\mathbf{s}_1^*,\mathbf{s}_2^*)}{M_{\oplus}(\Lambda_n,\mathbf{s}_1^*,\mathbf{s}_2^*)}\leq 4\frac{V'_{\oplus}}{V_{\oplus}}$.

Proof.

Let us define the following sets, $F_n = \left\{ \mathbf{s}_1 \in \mathcal{V}_n : M_1(\Lambda_n, \mathbf{s}_1) \geq \frac{V_n(\sqrt{nP})}{8\det(\Lambda_n)} \right\}, G_n = \left\{ \mathbf{s}_2 \in \mathcal{V}_n : M_2(\Lambda_n, \mathbf{s}_2) \geq \frac{V_n(\sqrt{nP})}{8\det(\Lambda_n)} \right\}$ and $O_n = \left\{ (\mathbf{s}_1, \mathbf{s}_2) \in \mathcal{V}_n \times \mathcal{V}_n : \frac{M'_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2)}{M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2)} \leq 4\frac{V'_\oplus}{V_\oplus} \right\}$.

Therefore $\mathcal{V}_n^* = (F_n \times G_n) \bigcap O_n$. Also, we define O_n^C and $(F_n \times G_n)^C$ as $O_n^C = (\mathcal{V}_n \times \mathcal{V}_n) \backslash O_n$ and $(F_n \times G_n)^C = (\mathcal{V}_n \times \mathcal{V}_n) \backslash (F_n \times G_n)$. Hence,

$$\mathcal{V}_n \times \mathcal{V}_n = \mathcal{V}_n^* \bigcup \left\{ (F_n \times G_n) \cap O_n^C \right\} \bigcup \left\{ (F_n \times G_n)^C \right\} \tag{4.34}$$

From corollary J.1, we have

$$V_\oplus = \int_{\mathcal{V}_n \times \mathcal{V}_n} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) \tag{4.35}$$

$$\begin{aligned} V_\oplus \leq & \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \int_{O_n^C} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) \\ & + \int_{(F_n \times G_n)^C} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2). \end{aligned}$$

We can replace the second integral, using the condition that the translations are not in the set O_n, to get a bound on $M_\oplus$ as shown below,

$$\begin{aligned} V_\oplus \leq & \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4V'_\oplus} \int_{O_n^C} M'_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) \\ & + \int_{(F_n \times G_n)^C} \left(\sum_{h_1 \in \Lambda_n} \sum_{h_2 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_1 + \mathbf{s}_1) \chi_{T_{\sqrt{P}}}(h_2 + \mathbf{s}_2) \right) dV(\mathbf{s}_1) dV(\mathbf{s}_2). \end{aligned}$$

Since, $O_n^C \subset \mathcal{V}_n \times \mathcal{V}_n$, we can bound the second integral again as shown below.

$$\begin{aligned} V_\oplus \leq & \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4V'_\oplus} \int_{\mathcal{V}_n \times \mathcal{V}_n} M'_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) \\ & + \int_{(F_n \times G_n)^C} \left(\sum_{h_1 \in \Lambda_n} \sum_{h_2 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_1 + \mathbf{s}_1) \chi_{T_{\sqrt{P}}}(h_2 + \mathbf{s}_2) \right) dV(\mathbf{s}_1) dV(\mathbf{s}_2). \end{aligned}$$

Using the expression for $V'_\oplus$ from corollary J.1, we can simplify the integral in the second term as given below.

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + \int_{(F_n \times G_n)^C} \left(\sum_{h_1 \in \Lambda_n} \sum_{h_2 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_1 + \mathbf{s}_1) \chi_{T_{\sqrt{P}}}(h_2 + \mathbf{s}_2) \right) dV(\mathbf{s}_1) dV(\mathbf{s}_2).$$

Next we change the double summation for the third term into a product of two summations to get

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + \int_{(F_n \times G_n)^C} \left(\sum_{h_1 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_1 + \mathbf{s}_1) \right) \left(\sum_{h_2 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_2 + \mathbf{s}_2) \right) dV(\mathbf{s}_1) dV(\mathbf{s}_2).$$

The summation $\sum_{h_1 \in \Lambda_n} \chi_{T_{\sqrt{P}}}(h_1 + \mathbf{s}_1)$ can be seen to count the number of lattice points in the sphere $T_{\sqrt{P}}$, for the translation $\mathbf{s}_1$. This is by definition equivalent to $M(\Lambda_n, \mathbf{s}_1)$. Similarly we can replace the other summation by $M(\Lambda_n, \mathbf{s}_2)$, to get

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + \int_{(F_n \times G_n)^C} M(\Lambda_n, \mathbf{s}_1) M(\Lambda_n, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2).$$

Since $(F_n \times G_n)^C \subset (F_n \times \mathcal{V}_n) \cup (\mathcal{V}_n \times G_n)$ we can bound the integral to get

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + \int_{(F_n^C \times \mathcal{V}_n)} M(\Lambda_n, \mathbf{s}_1) M(\Lambda_n, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \int_{(\mathcal{V}_n \times G_n^C)} M(\Lambda_n, \mathbf{s}_1) M(\Lambda_n, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2).$$

We next use Blichfeldt's principle to simplify the integrals.

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + V_n(\sqrt{nP}) \int_{F_n^C} M(\Lambda_n, \mathbf{s}_1) dV(\mathbf{s}_1) + V_n(\sqrt{nP}) \int_{G_n^C} M(\Lambda_n, \mathbf{s}_2) dV(\mathbf{s}_2).$$

We use the condition $\mathbf{s}_1 \notin F_n$ and $\mathbf{s}_2 \notin G_n$, to get

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + V_n(\sqrt{nP}) \frac{V_n(\sqrt{nP})}{8\det(\Lambda_n)} \int_{F_n^C} dV(\mathbf{s}_1)$$
$$+ V_n(\sqrt{nP}) \frac{V_n(\sqrt{nP})}{8\det(\Lambda_n)} \int_{G_n^C} dV(\mathbf{s}_2).$$

Since $F_n^C, G_n^C \subset \mathcal{V}_n$ and $\int_{\mathcal{V}_n} dV(\mathbf{s}_1), \int_{\mathcal{V}_n} dV(\mathbf{s}_2) = \det(\Lambda_n)$, we obtain,

$$V_\oplus \leq \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2) + \frac{V_\oplus}{4} + V_n(\sqrt{nP}) \frac{V_n(\sqrt{nP})}{8}$$
$$+ V_n(\sqrt{nP}) \frac{V_n(\sqrt{nP})}{8}.$$

Finally using $V_\oplus = (V_n(\sqrt{nP}))^2$, we obtain

$$V_\oplus \leq 2 \int_{\mathcal{V}_n^*} M_\oplus(\Lambda_n, \mathbf{s}_1, \mathbf{s}_2) dV(\mathbf{s}_1) dV(\mathbf{s}_2).$$

This implies that the measure of $\mathcal{V}_n^*$ must be non-zero and hence, there must be at least some translations $(\mathbf{s}_1^*, \mathbf{s}_2^*)$ of the lattice, where the requirements of the lemma hold. $\square$

5. Minkowski-Hlawka theorem to show existence of good lattices

Lemma J.5. *There exists a good lattice* Λ_n^* *and translational vectors* $\mathbf{s}_1^*$, $\mathbf{s}_2^*$ *such that the following holds*

$$\frac{1}{M_\oplus(\Lambda_n^*, \mathbf{s}_1^*, \mathbf{s}_2^*)} \sum_{(\mathbf{x}_1, \mathbf{x}_2) \in \mathcal{C}_\oplus^\triangle} \sum_{g \in \Lambda_n^* \setminus \{0\}} p_\theta\left(\mathbf{x}_1 + \mathbf{x}_2, g + \mathbf{x}_1 + \mathbf{x}_2\right) \chi_{T^\triangle_{\sqrt{2P}}}(g + \mathbf{x}_1 + \mathbf{x}_2)$$
$$\leq \frac{2(n-1)\pi^{\frac{n-1}{2}} (n(2P+\delta))^{n/2}}{d_n n \Gamma(\frac{n+1}{2})} \int_0^\theta \sin^{n-2}(x) dx$$

and $M_1(\Lambda_n^*, \mathbf{s}_1^*) \geq \frac{V_n(\sqrt{nP})}{8 det(\Lambda_n^*)}$; $M_2(\Lambda_n^*, \mathbf{s}_2^*) \geq \frac{V_n(\sqrt{nP})}{8 det(\Lambda_n^*)}$; $\frac{M'_\oplus(\Lambda_n^*, \mathbf{s}_1^*, \mathbf{s}_2^*)}{M_\oplus(\Lambda_n^*, \mathbf{s}_1^*, \mathbf{s}_2^*)} \leq 4 \frac{V'_\oplus}{V_\oplus}$, *where* $p_\theta(\mathbf{x}, \mathbf{x}') \stackrel{\triangle}{=} Pr(\pi(\mathbf{x}) + Z^n \notin B_\theta(\mathbf{x}'))$.

Proof. First let us define the function $f(z)$ as follows

$$f(\mathbf{z}) = \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} p_\theta\left(\mathbf{u}+\mathbf{v},\mathbf{z}+\mathbf{u}+\mathbf{v}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(g+\mathbf{u}+\mathbf{v})\chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{v})\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v})$$
$$dV(\mathbf{u})dV(\mathbf{v})$$

Clearly $f(z)$ is a nonnegative integrable function and has bounded support. Hence we can apply Minkowski-Hlawka theorem and find a lattice Λ_n^*, with $\det(\Lambda_n^*) = d_n$ such that

$$\sum_{g\in\Lambda_n^*\setminus\{0\}} f(g) \leq \frac{1}{d_n}\int_{\mathbb{R}^n} f(\mathbf{z})dV(\mathbf{z}).$$

Consider the integral I defined below as,

$$I \triangleq \int_{\mathcal{V}_n^*}\sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{C}_{\oplus}^{\Delta}}\sum_{g\in\Lambda_n^*\setminus\{0\}} p_\theta\left(\mathbf{x}_1+\mathbf{x}_2,g+\mathbf{x}_1+\mathbf{x}_2\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(g+\mathbf{x}_1+\mathbf{x}_2)dV(\mathbf{s}_1)dV(\mathbf{s}_2) \tag{4.36}$$
$$\leq \int_{\mathcal{V}_n\times\mathcal{V}_n}\sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{C}_{\oplus}^{\Delta}}\sum_{g\in\Lambda_n^*\setminus\{0\}} p_\theta\left(\mathbf{x}_1+\mathbf{x}_2,g+\mathbf{x}_1+\mathbf{x}_2\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(g+\mathbf{x}_1+\mathbf{x}_2)dV(\mathbf{s}_1)dV(\mathbf{s}_2).$$

The above follows as $\mathcal{V}_n^* \subseteq \mathcal{V}_n\times\mathcal{V}_n$.

$$I \leq \int_{\mathcal{V}_n\times\mathcal{V}_n}\sum_{(\mathbf{h}_1,\mathbf{h}_2)\in\Lambda_n^*\times\Lambda_n^*}\sum_{g\in\Lambda_n^*\setminus\{0\}} p_\theta\left(h_1+\mathbf{s}_1+h_2+\mathbf{s}_2,g+h_1+\mathbf{s}_1+h_2+\mathbf{s}_2\right)$$
$$\times\chi_{T^{\Delta}_{\sqrt{2P}}}(g+h_1+\mathbf{s}_1+h_2+\mathbf{s}_2)\chi_{T_{\sqrt{P}}}(h_1+\mathbf{s}_1)$$
$$\times\chi_{T_{\sqrt{P}}}(h_2+\mathbf{s}_2)\chi_{T^{\Delta}_{\sqrt{2P}}}(h_1+\mathbf{s}_1+h_2+\mathbf{s}_2)dV(\mathbf{s}_1)dV(\mathbf{s}_2).$$

In the above equation we substituted $\mathbf{x}_1 = h_1+\mathbf{s}_1$ and $\mathbf{x}_2 = h_2+\mathbf{s}_2$. Next applying Blichfeldt's principle twice we obtain,

$$I \leq \int_{\mathbb{R}^n}\int_{\mathbb{R}^n}\sum_{g\in\Lambda_n^*\setminus\{0\}} p_\theta\left(\mathbf{u}+\mathbf{v},g+\mathbf{u}+\mathbf{v}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(g+\mathbf{u}+\mathbf{v})\chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{v})$$
$$\times\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v})dV(\mathbf{u})dV(\mathbf{v}).$$

Here $\mathbf{u} = h_1+\mathbf{s}_1$ and $\mathbf{v} = h_2+\mathbf{s}_2$. We can next take the summation outside the double integral, as we are dealing with a finite number of non-zero sums. This gives,

$$I \leq \sum_{g\in\Lambda_n^*\setminus\{0\}} \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} p_\theta\left(\mathbf{u}+\mathbf{v}, g+\mathbf{u}+\mathbf{v}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(g+\mathbf{u}+\mathbf{v})\chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{v})$$

$$\times\, \chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v})dV(\mathbf{u})dV(\mathbf{v}).$$

Next we use Minkowski-Hlawka theorem to establish that there exists at least one lattice Λ_n^* such that the summation can be bounded by an integral, as shown below. In short Minkowski-Hlawka theorem gives an existence result that such a lattice can be found, but does not give a way to find such a lattice.

$$I \leq \frac{1}{d_n}\int\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} p_\theta\left(\mathbf{u}+\mathbf{v}, \mathbf{w}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{w})\chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{v})$$

$$\times\, \chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v})dV(\mathbf{u})dV(\mathbf{v})dV(\mathbf{w}).$$

In the above we have replaced $g+\mathbf{u}+\mathbf{v}$ with $\mathbf{w}$. Again we change the order of integration to get,

$$I \leq \frac{1}{d_n}\int_{\mathbb{R}^n}\int_{\mathbb{R}^n}\left[\int p_\theta\left(\mathbf{u}+\mathbf{v}, \mathbf{w}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{w})dV(\mathbf{w})\right]$$

$$\times\, \chi_{T_{\sqrt{P}}}(\mathbf{u})\chi_{T_{\sqrt{P}}}(\mathbf{v})\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{u}+\mathbf{v})dV(\mathbf{u})dV(\mathbf{v}).$$

The inner integral can be seen to be independent of $\mathbf{u}+\mathbf{v}$, and the outer integral can be seen to be lesser than $V_\oplus$. Hence we can express the resultant integral as,

$$I \leq \frac{V_\oplus}{d_n}\int p_\theta\left(\mathbf{s}_0, \mathbf{w}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{w})dV(\mathbf{w}).$$

Hence we next evaluate the integral using similar steps as in [50], first by changing to spherical coordinates.

$$I \leq \frac{V_\oplus}{d_n}\int_{\sqrt{n(2P-\delta)}}^{\sqrt{n(2P+\delta)}}\left[\int_{\mathbf{w}:\|\mathbf{w}\|=r} p_\theta\left(\mathbf{s}_0, \mathbf{w}\right)\chi_{T^{\Delta}_{\sqrt{2P}}}(\mathbf{w})dA(\mathbf{w})\right]dr,$$

where $dA(\mathbf{w})$ is the $(n-1)$-dimensional volume element of a thin spherical element at a distance r from the origin. Next we use the definition of p_θ to get,

$$I \leq \frac{V_\oplus}{d_n} \int_{\sqrt{n(2P-\delta)}}^{\sqrt{n(2P+\delta)}} \left[\int_{\mathbf{w}:\|\mathbf{w}\|=r} \Pr\left(\pi(\mathbf{s}_0) + Z^n \in B_\theta(\mathbf{w})\right) \chi_{T^\Delta_{\sqrt{2P}}}(\mathbf{w}) dA(\mathbf{w}) \right] dr.$$

We evaluate the probability by conditioning on Z^n.

$$I \leq \frac{V_\oplus}{d_n} \int_{\sqrt{n(2P-\delta)}}^{\sqrt{n(2P+\delta)}} \left[\int_{\mathbf{w}:\|\mathbf{w}\|=r} \left[\int \Pr\left(\pi(\mathbf{s}_0) + Z^n \in B_\theta(\mathbf{w}) | Z^n = \mathbf{z}\right) \Pr(Z^n = \mathbf{z}) dV(\mathbf{z}) \right] \times \chi_{T^\Delta_{\sqrt{2P}}}(\mathbf{w}) dA(\mathbf{w}) \right] dr.$$

Since the function is non-negative, the order of integration can be interchanged to obtain

$$I \leq \frac{V_\oplus}{d_n} \int \left[\int_{\sqrt{n(2P-\delta)}}^{\sqrt{n(2P+\delta)}} \int_{\mathbf{w}:\|\mathbf{w}\|=r} \left[\Pr\left(\pi(\mathbf{s}_0) + Z^n \in B_\theta(\mathbf{w}) | Z^n = \mathbf{z}\right)\right] \chi_{T^\Delta_{\sqrt{2P}}}(\mathbf{w}) dA(\mathbf{w}) dr \right] \Pr(Z^n = \mathbf{z}) dV(\mathbf{z}).$$

Due to the conditioning on Z^n, the conditional probability becomes deterministic and is equivalent to the cross sectional area of a hypercone of half-angle θ, intersecting with a hypersphere of radius r. Note that in the result in [50], the area of cross section must be a function of r and not of $\sqrt{n(2P-\delta)}$. This gives,

$$I \leq \frac{V_\oplus}{d_n} \left[\int \Pr(Z^n = \mathbf{z}) dV(\mathbf{z}) \right] \int_{\sqrt{n(2P-\delta)}}^{\sqrt{n(2P+\delta)}} \left[\frac{(n-1)\pi^{\frac{n-1}{2}} r^{n-1}}{\Gamma(\frac{n+1}{2})} \int_0^\theta \sin^{n-2}(x) dx \right] dr.$$

This in turn yields

$$I \leq \frac{V_\oplus}{d_n} \left[\frac{(n-1)\pi^{\frac{n-1}{2}} \left((n(2P+\delta))^{n/2} - (n(2P-\delta))^{n/2} \right)}{n\Gamma(\frac{n+1}{2})} \int_0^\theta \sin^{n-2}(x) dx \right].$$

$$I \leq \frac{V_\oplus}{d_n} \left[\frac{(n-1)\pi^{\frac{n-1}{2}} (n(2P+\delta))^{n/2}}{n\Gamma(\frac{n+1}{2})} \int_0^\theta \sin^{n-2}(x) dx \right].$$

Next using Lemma J.4 we can bound the resultant integral to get,

$$I \leq 2 \int_{\mathcal{V}_n^*} M_{\oplus}(\Lambda_n^*, \mathbf{s}_1, \mathbf{s}_2) \left[\frac{(n-1)\pi^{\frac{n-1}{2}}(n(2P+\delta))^{n/2}}{d_n n \Gamma(\frac{n+1}{2})} \int_0^{\theta} \sin^{n-2}(x) dx \right] dV(\mathbf{s}_1) dV(\mathbf{s}_2). \tag{4.37}$$

Now comparing (4.36) and (4.37), and also knowing that the measure of $\mathcal{V}_n^*$ is non-zero, we can see that there must be at least one such translational vector pair $(\mathbf{s}_1^*, \mathbf{s}_2^*)$ such that the required assertion of the lemma holds. □

CHAPTER V

EXTENSIONS AND RESULTS FOR FADING CHANNELS

In this chapter, we will study some extensions of the bi-directional relaying problem. One extension we consider is the fading channel scenario where the channel gains are not symmetric. Another extension we consider is the multi-hop case. We next present some related prior work.

A. Related prior work

There has been some recent work on the bi-directional relay problem with asymmetric channel gains. In [41], several schemes including compress and forward, amplify and forward, decode and forward and mixed forward have been suggested. There has also been some interesting work on using nested lattices for asymmetric channel gains in [42, 55]. In [42], a scheme that is optimal at high signal-to-noise ratios (snr) is given for a given realization of the asymmetric channel. This scheme uses lattices with different rates at each node for the MAC phase, while the broadcast phase uses a random coding scheme discussed in [56].

In contrast to [42], in this chapter we are interested in proposing power allocation policies for exchanging information through a fading channel and also we are interested in reduced complexity schemes that perform very close to the upper bound. We use symmetric nested lattices at the two nodes, i.e., both the nodes use the same lattice code having the same rate. Also the relay node during the broadcast phase uses the same lattice and does not require a random code, which will have implications in reducing the complexity of the encoding/decoding scheme. Hence we show that for a fading scenario, it is possible to design schemes that can perform very close to the upper bound at a reduced complexity. However for certain scenarios, the scheme presented in [42] can outperform the scheme presented here.

B. Main results and comments

Before introducing our proposed schemes, we will first briefly state the main results.

- We consider a bi-directional relay where two nodes wish to exchange information with each other through a relay. The transmission is assumed to occur over L coherence time intervals and the fading channel coefficients are assumed to be known to all the nodes. The channel gains are assumed to be reciprocal, i.e. the uplink channel gains is the same as the down link channel gains. The system model is presented in detail in section C. An upper bound on the exchange rate is setup as a convex optimization problem for the above problem and this is discussed in section D.

- A scheme is proposed which at high SNRs, performs away from the upper bound by at most 0.09 bits(see Theorem F.3). The scheme uses nested lattice encoding and the transmit power is chosen to be inversely proportional to the channel gains.

- A multi-hop case is considered and for symmetric channel gains, it is shown that the upper bound on the exchange rate can be obtained at high SNRs. This is discussed in section G.

C. System model and problem statement

We study a simple 3-node linear Gaussian network, with asymmetric channel gains as shown in Fig. 21. Node A and node B wish to exchange information between each other through the relay node R. However, nodes A and B cannot communicate with

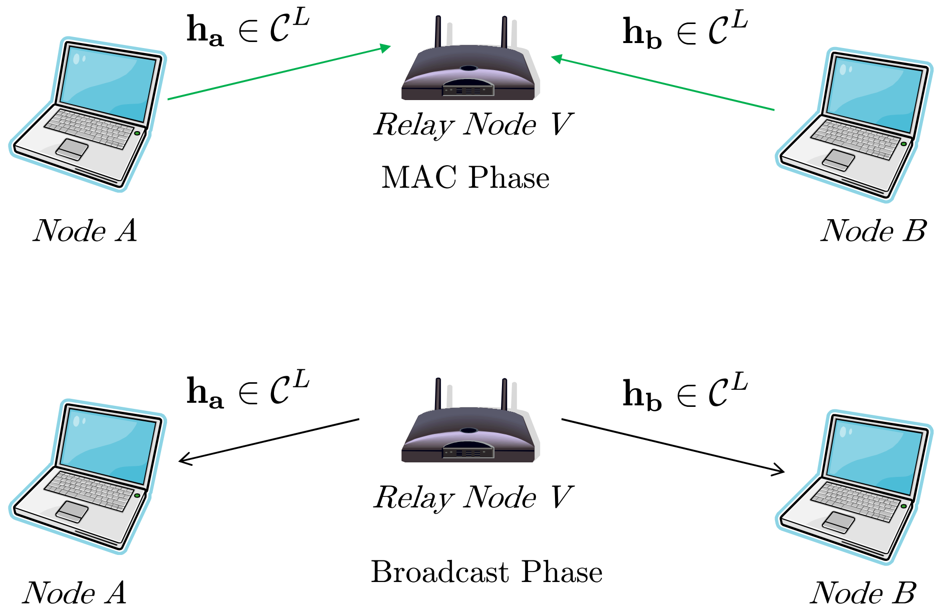

Fig. 21. Problem setup with fading links h_a and h_b.

each other directly. The nodes are assumed to be half-duplex, i.e. a node can not transmit and listen at the same time. We use the block fading model to model the channels between the nodes and the relay. The channel gains between the nodes and the relays remain constant over a coherence time interval. It is assumed that the transmission happens over L such coherence time intervals. Each coherence interval corresponds to N uses of the channel. Hence, effectively NL uses of the channel are available for communication. For the channel between the node A and the relay R, each of the coefficients of the L length vector $\mathbf{h_{ar}} \in \mathbb{C}^L$, represent the channel gain for each coherence time interval. Similarly the channel between the node B and the relay R, the relay R and node A, and the relay R and node B, are captured by the channel gain vectors $\mathbf{h_{br}}$, $\mathbf{h_{ra}}$ and $\mathbf{h_{rb}} \in \mathbb{C}^L$ respectively(vectors are denoted by bold face letters such as $\mathbf{v}$ throughout the paper). The channels are assumed to be reciprocal, i.e., $\mathbf{h_{ar}} = \mathbf{h_{ra}} := \mathbf{h_a}$ and $\mathbf{h_{br}} = \mathbf{h_{rb}} := \mathbf{h_b}$.

Let $\mathbf{u}_A \in \{0,1\}^{k_a L}$ and $\mathbf{u}_B \in \{0,1\}^{k_b L}$ be the information vectors at nodes A and B. We assume a protocol where the communication takes place in two phases at each coherence time interval i ($i \in \{1, 2 \ldots L\}$). The phases are the multiple access (MAC) phase and the broadcast phase. $\Delta \in [0,1]$ is the fraction of channel uses for which the MAC phase is used and $(1-\Delta)$ is the fraction of channel uses for which the broadcast phase is used. It is assumed that communication in the MAC and broadcast phases are orthogonal. For example, this could be in two separate frequency bands (or in two different time slots) and hence the MAC phase and broadcast phase do not interfere with each other.

MAC phase: During the MAC phase of each coherence time interval i, nodes A and B transmit while the relay node listens. $\mathbf{x_{ai}} \in \mathbb{C}^{\Delta N}$ and $\mathbf{x_{bi}} \in \mathbb{C}^{\Delta N}$ are the transmitted vectors at nodes A and B, respectively. The MAC phase takes place in ΔN uses of the complex additive white Gaussian noise (AWGN) channel. Further it is assumed that the two transmissions are perfectly synchronized. Hence the received signal at the relay $\mathbf{y_{ri}} \in \mathbb{C}^{\Delta N}$, is given by

$$\mathbf{y_{ri}} = h_{ai}\mathbf{x_{ai}} + h_{bi}\mathbf{x_{bi}} + \mathbf{z_{ri}},$$

where the components of $\mathbf{z_{ri}} \in \mathbb{C}^{\Delta N}$ are independent identically distributed (i.i.d) complex, circularly symmetric Gaussian random variables with zero mean and unit variance. The average transmit power at the nodes A and B in the i^{th} coherence time interval is given as $E[||X_{ai}||^2] = P_{ai}$ and $E[||X_{bi}||^2] = P_{bi}$.

Broadcast phase: During the broadcast phase, the relay transmits $\mathbf{x_{ri}} \in \mathbb{C}^{(1-\Delta)N}$ in the i^{th} coherence time interval to both nodes A and B. The nodes A and B receive

$\mathbf{y_{ai}}$ and $\mathbf{y_{bi}}$, respectively where

$$\begin{aligned}\mathbf{y_{ai}} &= h_{ai}\mathbf{x_{ai}} + \mathbf{z_{ai}} \\ \mathbf{y_{bi}} &= h_{bi}\mathbf{x_{bi}} + \mathbf{z_{bi}}.\end{aligned}$$

The average transmit power at the relay node during the i^{th} coherence time interval is given by P_{ri}, and the receiver noise at the two nodes is complex Gaussian with zero mean and unit variance.

Further, it is assumed that there is a total sum power constraint over all the nodes. Since the MAC phase is used during the fraction Δ and the broadcast phase is used during the fraction $(1-\Delta)$ of the available time slots, the total power constraint is expressed as

$$\frac{\Delta}{L}\sum_{i=1}^{L} P_{ai} + \frac{\Delta}{L}\sum_{i=1}^{L} P_{bi} + \frac{(1-\Delta)}{L}\sum_{i=1}^{L} P_{ri} \leq P.$$

We are interested in power allocation strategies and good encoding/decoding schemes that maximize the amount of information (maximize $k_a/(LN)+k_b/(LN)$) that can be exchanged reliably (such that the probability of error can be made arbitrarily small in the limit of $N \to \infty$). We refer to the maximum value of $k_a/(LN)+k_b/(LN)$ that can be reliably exchanged with a given scheme as the exchange rate for that scheme. The exchange capacity is then the supremum of all such rates over the encoding schemes.

D. Upper bound for the two phase protocol

We can easily obtain an upper bound for the two phase protocol using cut-set arguments and as in [41]. In our problem model the channel remains constant in each coherence time interval. Hence, the channel over L such coherence time intervals can be modeled as a set of L parallel channels. At each coherence time interval i, the maximum information rate that can be transmitted from node A to node B is bounded by the minimum of the information capacity from node A to relay node R, and relay node R to node B. This can be expressed as $\min\{\Delta C(|h_{ai}|^2 P_{ai}), (1-\Delta) C(|h_{bi}|^2 P_{ri})\}$, where $C(x) := \log(1+x)$. Here Δ is the fraction of time node A transmits and $(1-\Delta)$ is the fraction of time the relay node transmits. Similarly the rate that can be transmitted from node B to node A is bounded by the minimum of the information capacity from node B to relay R and from relay R to node A, which can be expressed as $\min\{\Delta C(|h_{bi}|^2 P_{bi}), (1-\Delta) C(|h_{ai}|^2 P_{ri})\}$. Hence the total rate that can be transmitted over L such coherence time intervals can be expressed as the sum of the rates at each coherence time interval. Combining the above, the upper bound on the exchange capacity can be expressed as the solution of an optimization problem given by,

$$
\begin{aligned}
\text{maximize} \quad & \frac{1}{L}\sum_{i=1}^{L} \min\{\Delta C(|h_{ai}|^2 P_{ai}), (1-\Delta) C(|h_{bi}|^2 P_{ri})\} \\
& + \frac{1}{L}\sum_{i=1}^{L} \min\{\Delta C(|h_{bi}|^2 P_{bi}), (1-\Delta) C(|h_{ai}|^2 P_{ri})\} \qquad (5.1) \\
\text{subject to} \quad & \frac{\Delta}{L}\sum_{i=1}^{L} P_{ai} + \frac{\Delta}{L}\sum_{i=1}^{L} P_{bi} + \frac{(1-\Delta)}{L}\sum_{i=1}^{L} P_{ri} \le P \\
& P_{ai}, P_{bi}, P_{ri} \ge 0, i \in 1, 2 \ldots L.
\end{aligned}
$$

Since Δ is fixed, we can see that the objective function given above is concave and also the constraints form a convex set. Hence convex optimization techniques can be easily applied to this setup to get the optimal solution for the above convex problem.

E. Proposed scheme using channel inversion and lattice coding

In this section we discuss our achievable scheme based on nested lattice decoding by Erez and Zamir[46]. The proposed scheme follows closely the lattice coding scheme for the symmetric case discussed in the previous chapter. We observed that suppose each of the nodes A, B and the relay R, has the same power constraint (say P_Λ), then at high signal to noise ratios, a rate close to the upper bound $C(P_\Lambda)$ can be exchanged. In other words, the nested lattice coding approach works best when the receiver channel signal strengths from the two nodes are the same.

In our proposed scheme, we enforce $|h_{ai}|^2 P_{ai} = |h_{bi}|^2 P_{bi}$ for every i^{th} coherence time interval in the MAC phase. This means that each node uses a coarse lattice of power $P_{\Lambda i}$, and each node performs a channel inversion at the transmitter, so that the relay receives equal signal strengths from both the nodes. For the broadcast phase, to ensure that the nodes A and B can decode the message from the relay, we enforce that transmit power at the relay is always larger than the transmit power at the nodes, or $P_{ri} \geq P_{ai}, P_{bi}$.

First let us explain our achievable scheme in detail for the i^{th} coherence interval with known channel gains h_{ai}, h_{bi}. We first obtain the power allocation profiles P_{ai}, P_{bi} and P_{ri}, based on the additional requirements of $|h_{ai}|^2 P_{ai} = |h_{bi}|^2 P_{bi}$ and $P_{ri} \geq P_{ai}, P_{bi}$. The allocation is discussed in more detail later in the section. Let us next define $P_{\Lambda i} := |h_{ai}|^2 P_{ai} = |h_{bi}|^2 P_{bi}$ and for each coherence time interval i, choose a nested lattice structure having a fine lattice Λ_i^f with a coarse lattice Λ_i nested in it. The second moment per unit dimension of the coarse lattice is $P_{\Lambda i}/2$. Also the channel model considered in this problem setup has complex inputs and complex noise, when compared to the real Gaussian channel model in [40]. The complex channel provides two degrees of freedom. To take advantage of this we can perform nested lattice coding separately along the in-phase and the quadrature phase components. In all the vectors discussed below namely $\mathbf{x_{ai}}, \mathbf{x_{bi}}, \mathbf{t_{ai}}, \mathbf{t_{bi}}, \mathbf{u_{ai}}$ and $\mathbf{u_{bi}}$ are complex vectors and can be expressed as the complex sum of their in-phase and quadrature phase components. For example $\mathbf{x_{ai}}$ can be expressed as $\mathrm{Re}\{\mathbf{x_{ai}}\} + \jmath \mathrm{Im}\{\mathbf{x_{ai}}\}$.

First at each coherence interval i during the MAC phase, the data at the nodes A

and B are mapped to lattice points $\mathbf{t_{ai}}$ and $\mathbf{t_{bi}}$ respectively. Let $\mathbf{u_{ai}}$ and $\mathbf{u_{bi}}$ be dithers that are uniformly distributed over the coarse lattice. The in-phase component of the dither and the quadrature phase component are independent of each other and each distributed uniformly in the coarse lattice Λ_i, with second moment $P_{\Lambda i}$. An output $(\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i$ is obtained at node A and $(\mathbf{t_{bi}} - \mathbf{u_{bi}}) \mod \Lambda_i$ at node B. Here $\mathbf{t_i} \mod \Lambda_i$ represents $(\mathrm{Re}\{\mathbf{t_i}\} \mod \Lambda_i) + \jmath(\mathrm{Im}\{\mathbf{t_i}\} \mod \Lambda_i)$.

Hence the transmitted vector $\mathbf{x_{ai}}$ at node A is given by,

$$\mathbf{x_{ai}} = \frac{(\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i}{h_{ai}} \tag{5.2}$$

Here the numerator $(\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i$ is the sum of the in-phase and quadrature phase components, expressed as $\mathrm{Re}(\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i + \jmath\mathrm{Im}(\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i$. Hence the second moment of the numerator per unit dimension is $P_{\Lambda i}/2 + P_{\Lambda i}/2 = P_{\Lambda i}$. Hence the average transmit power on $\mathbf{x_{ai}}$ is $P_{\Lambda i}/|h_{ai}|^2 = P_{ai}$. Thus we meet the average power constraint of P_{ai} at node A. Similarly the transmitted vector $\mathbf{x_{bi}}$ at node B is given below. This also meets the average power constraint P_{bi}.

$$\mathbf{x_{bi}} = \frac{(\mathbf{t_{bi}} - \mathbf{u_{bi}}) \mod \Lambda_i}{h_{bi}} \tag{5.3}$$

The relay receives

$$\mathbf{y_{ri}} = h_{ai}\mathbf{x_{ai}} + h_{bi}\mathbf{x_{bi}} + \mathbf{z_{ri}} \tag{5.4}$$

or

$$\mathbf{y_{ri}} = (\mathbf{t_{ai}} - \mathbf{u_{ai}}) \mod \Lambda_i + (\mathbf{t_{bi}} - \mathbf{u_{bi}}) \mod \Lambda_i + \mathbf{z_{ri}} \tag{5.5}$$

The decoder next forms $(\alpha_i \mathbf{y_{ri}} + \mathbf{u_{ai}} + \mathbf{u_{bi}}) \mod \Lambda_i$ and performs nested lattice decoding and decodes to $\mathbf{t_{ri}} = (\mathbf{t_{ai}} + \mathbf{t_{bi}}) \mod \Lambda_i$ with high probability, as long as the transmission rate from each of the nodes is less than $2\{\frac{1}{2}\log(0.5 + P_{\Lambda_i})\}$. The factor 2 is present because the channel coefficients are complex and we have 2 degrees of freedom. Also, α_i is chosen as $\alpha_i = \frac{2P_{\Lambda_i}}{2P_{\Lambda_i}+1}$ and the steps involved in decoding to $\mathbf{t_{ri}}$ can be found in [40].

The relay next forms $(\mathbf{t_{ri}} - \mathbf{u_{ri}}) \mod \Lambda_i$ and during the broadcast phase transmits

$$\mathbf{x_{ri}} = \sqrt{\frac{P_{ri}}{P_{\Lambda_i}}}\{(\mathbf{t_{ri}} - \mathbf{u_{ri}}) \mod \mathbf{\Lambda_i}\} \tag{5.6}$$

Both the nodes A and B can decode to $\mathbf{t_{ri}}$ as $|h_{ai}|^2 P_{ri}, |h_{bi}|^2 P_{ri} \geq P_{\Lambda_i}$, since $P_{ri} \geq P_{ai}, P_{bi}$. Hence effectively a rate of $\frac{1}{2}\log(0.5 + P_{\Lambda i})$ can be exchanged by the nodes.

Also define $D(x) := u.c.e\{\log(0.5+x), 0.5\log(1+2x)\}, x \geq 0$. Here $u.c.e$ denotes the upper concave envelope of the two functions. Hence the optimization problem can be expressed as follows with a few more constraints added.

$$\begin{aligned}
\text{maximize} \quad & \frac{1}{L}\sum_{i=1}^{L} \min\{\Delta D(|h_{ai}|^2 P_{ai}), (1-\Delta) D(|h_{bi}|^2 P_{ri})\} \\
& + \frac{1}{L}\sum_{i=1}^{L} \min\{\Delta D(|h_{bi}|^2 P_{bi}), (1-\Delta) D(|h_{ai}|^2 P_{ri})\} \quad (5.7)\\
\text{subject to} \quad & \frac{\Delta}{L}\sum_{i=1}^{L} P_{ai} + \Delta \sum_{i=1}^{L} P_{bi} + \frac{(1-\Delta)}{L}\sum_{i=1}^{L} P_{ri} \leq P, \\
& |h_{ai}|^2 P_{ai} = |h_{bi}|^2 P_{bi}, \\
& P_{ri} \geq P_{ai}, \quad (5.8)\\
& P_{ri} \geq P_{bi}, \quad (5.9)\\
& P_{ai}, P_{bi}, P_{ri} \geq 0, i \in 1, 2 \ldots L
\end{aligned}$$

Fig. 22 shows some results obtained by numerically solving the optimization problems. Here we have $L = 100$, and the channel coefficients are taken from a Rayleigh distribution, and they have unit variance. For the channel coefficients we evaluate the average exchange rate per channel use, each for the upper bound, the lattice based scheme and also the amplify forward scheme. Fig. 22 shows that the

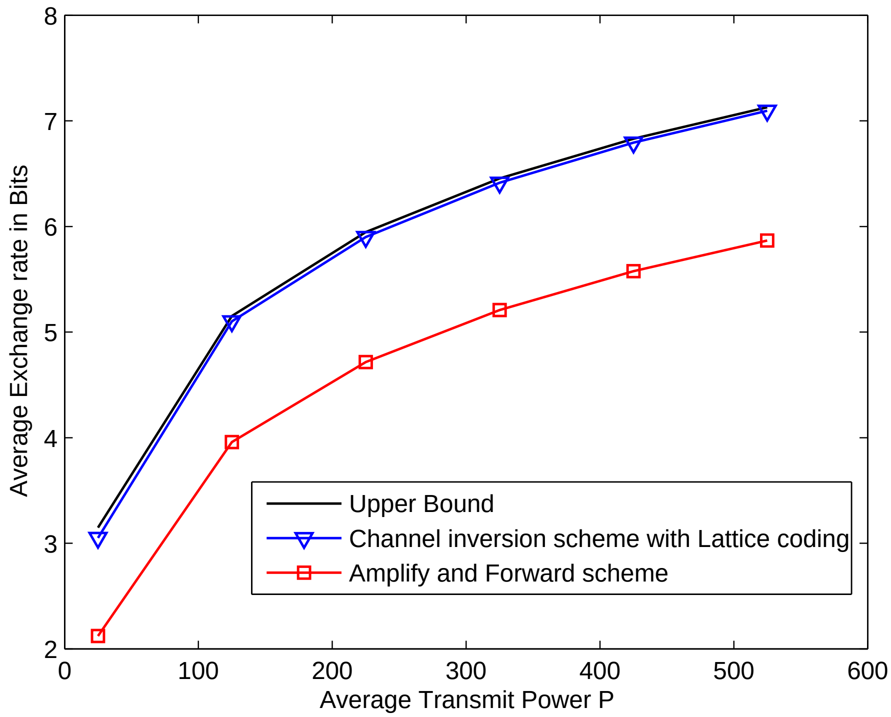

Fig. 22. Comparison of bounds for $\Delta = 0.5$.

exchange rate of our proposed scheme is very close to the upper bound. In the next section, to develop intuition about the numerical results, we present some analytical results for the same problem setup.

F. Analysis under high snr approximation

In this section we obtain analytical results for the power allocation strategy by solving the optimization problems (5.1) and (5.7). Though the optimization problems are convex, it is difficult to obtain analytical results for general snr. Hence, for ease of analysis, we solve the optimization problem under the *high snr approximation* which is defined as follows,

Definition F.1. *Using the high snr approximation implies that the functions* $C(x) := \log(1+x)$ *and* $D(x) := u.c.e\{\log(0.5+x), 0.5\log(1+2x)\}$ *are redefined with* $C(x) := \log(x)$ *and* $D(x) := \log(x)$*, respectively.*

We first analyze the upper bound as follows.

1. Upper bound

In the following theorem we solve the optimization problem for the upper bound given in (5.1) under the *high snr approximation*,

Theorem F.1. *For finite* L *and* $\Delta = 0.5$*, and under the high snr approximation, the optimal power allocation for the upper bound on the achievable rate for different ranges of* $\kappa_i^2 := |h_{ai}|^2/|h_{bi}|^2$ *is given by,*

Case 1 $0 < \kappa_i^2 <= \frac{-1+\sqrt{5}}{2}$,

$$P_{ai} = P \quad P_{bi} = P\frac{\kappa_i^2}{1+\kappa_i^2} \quad P_{ri} = P\frac{1}{1+\kappa_i^2}$$

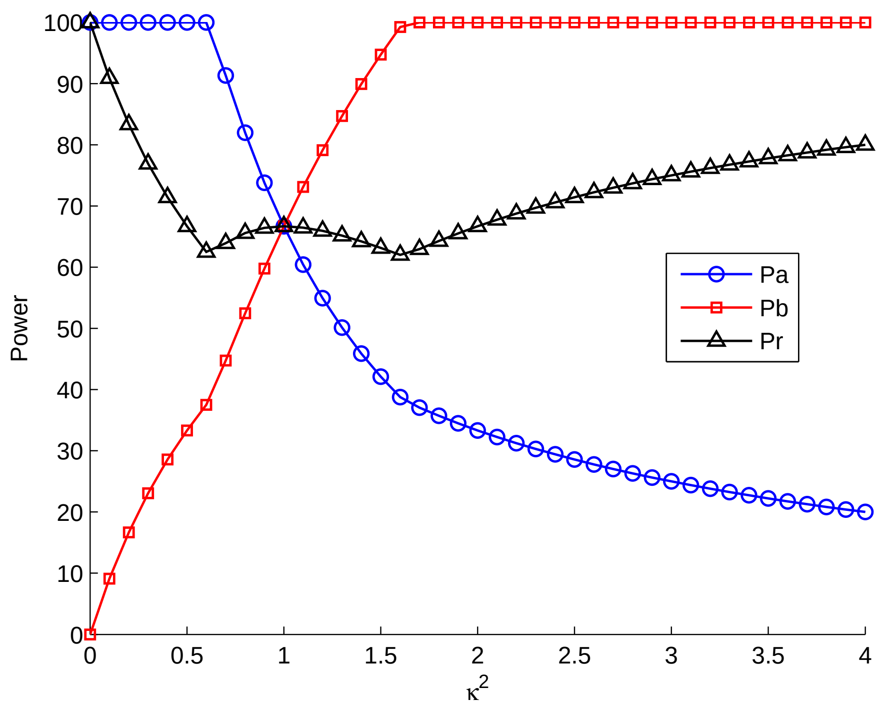

Fig. 23. Power allocation as a function of κ^2 for the upper bound.

Case 2 $\frac{-1+\sqrt{5}}{2} < \kappa_i^2 <= \frac{1+\sqrt{5}}{2}$,

$$P_{ai} = P\frac{2}{1+\kappa_i^2+\kappa_i^4} \quad P_{bi} = P\frac{2\kappa_i^4}{1+\kappa_i^2+\kappa_i^4} \quad P_{ri} = P\frac{2\kappa_i^2}{1+\kappa_i^2+\kappa_i^4}$$

Case 3 $\kappa_i^2 > \frac{1+\sqrt{5}}{2}$,

$$P_{ai} = P\frac{1}{1+\kappa_i^2} \quad P_{bi} = P \quad P_{ri} = P\frac{\kappa_i^2}{1+\kappa_i^2}$$

Proof. The problem can be solved analytically using the method of Lagrange multipliers and applying the Karush-Kuhn Tucker conditions as given below. The optimization problem for finite L and $\Delta = 0.5$ can be expressed below as,

$$\begin{aligned}
\text{maximize} \quad & \frac{1}{L}\sum_{i=1}^{L}\left(R_{ab}^{(i)} + R_{ba}^{(i)}\right) \\
\text{subject to} \quad & \frac{1}{2}C(|h_{ai}|^2 P_{ai}) > R_{ab}^{(i)}, \frac{1}{2}C(|h_{bi}|^2 P_{ri}) > R_{ab}^{(i)} \\
& \frac{1}{2}C(|h_{bi}|^2 P_{bi}) > R_{ba}^{(i)}, \frac{1}{2}C(|h_{ai}|^2 P_{ri}) > R_{ba}^{(i)} \\
& \frac{1}{L}\sum_{i=1}^{L}(P_{ai} + P_{bi} + P_{ri}) \leq 2P \\
& P_{ai}, P_{bi}, P_{ri} \geq 0, i \in \{1, 2 \dots L\}
\end{aligned}$$

We next use the *high snr approximation* $C(x) := \log x$ to simplify the analysis. The Lagrangian can then be expressed as,

$$\begin{aligned}
\mathcal{L} = & -\frac{1}{L}\sum_{i=1}^{L}\left(R_{ab}^{(i)} + R_{ba}^{(i)}\right) + \frac{\lambda}{L}\left(\sum_{i=1}^{L}(P_{ai} + P_{bi} + P_{ri}) - 2P\right) \\
& + \sum_{i=1}^{L}\mu_1^{(i)}(2R_{ab}^{(i)} - \log(|h_{ai}|^2 P_{ai})) + \sum_{i=1}^{L}\mu_2^{(i)}(2R_{ab}^{(i)} - \log(|h_{bi}|^2 P_{ri})) \\
& + \sum_{i=1}^{L}\mu_3^{(i)}(2R_{ba}^{(i)} - \log(|h_{bi}|^2 P_{bi})) + \sum_{i=1}^{L}\mu_4^{(i)}(2R_{ba}^{(i)} - \log(|h_{ai}|^2 P_{ri}))
\end{aligned}$$

Next taking the partial derivative of $\mathcal{L}$ with respect to each variable in $\mathcal{L}$ and equating to zero, gives us the following set of equations.

$$-\frac{1}{L}+2\mu_1^{(i)}+2\mu_2^{(i)}=0, -\frac{1}{L}+2\mu_3^{(i)}+2\mu_4^{(i)}=0$$

$$\frac{\lambda}{L}-\frac{\mu_1^{(i)}}{P_{ai}}=0, \frac{\lambda}{L}-\frac{\mu_3^{(i)}}{P_{bi}}=0, \frac{\lambda}{L}-\frac{\mu_2^{(i)}+\mu_4^{(i)}}{P_{ri}}=0$$

Solving for λ from the above set of equations gives $\lambda = \frac{1}{2P}$. Solving again the above set of equations for P_{ai}, P_{bi} and P_{ri} and together with the Karush-Kuhn Tucker(KKT) conditions, gives us the required power allocation as a function of κ_i^2. □

In the above proof, the parameter λ is not a function of the channel gains. This is so, since we have made the *high snr approximation*. This implies that the total power allocated $P_{ai}+P_{bi}+P_{ri}$, during each coherence time interval remains the same. However, the power in the individual nodes will vary based on the channel gains. From theorem 1, we can see that in case 1 we have at low κ_i^2, $\kappa_i^2 P_{ai} \approx P_{bi}$. In case 3, where $\kappa_i^2 >> 1$, $\kappa_i^2 P_{ai} \approx P_{bi}$. Also for case 2, where $\kappa_i^2 \approx 1$, $\kappa_i^2 P_{ai} \approx P_{bi}$. In other words this implies that $|h_{ai}|^2 P_{ai} \approx |h_{bi}|^2 P_{bi}$. This clearly suggests a channel inversion strategy which was presented in section E. An intuitive explanation for the channel inversion strategy can be given as follows. Let us consider a case where the channel gain from the node A to relay node is higher than the channel gain from the node B to the relay. The channel between the relay and node B becomes a bottleneck due its weaker gain. Hence it is better to reduce the transmit power at the node A and distribute it to the other nodes, which naturally suggests a channel inversion strategy. In the next section, we analyze our achievable scheme discussed in section E, under the *high snr approximation*.

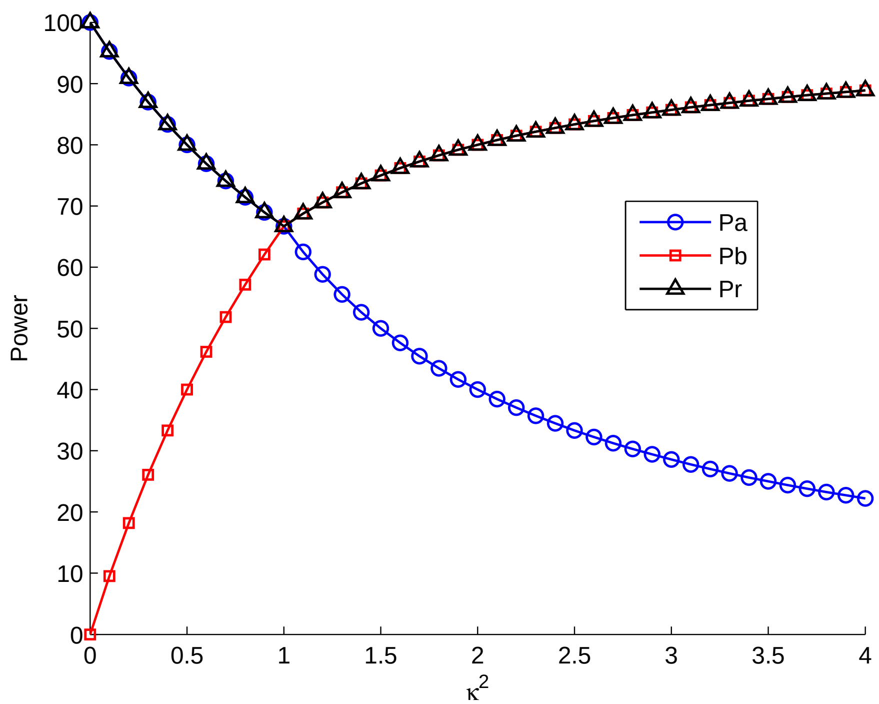

Fig. 24. Power allocation as a function of κ^2 for our proposed scheme.

2. Achievable rate of our proposed scheme

The optimization problem for the channel inversion scheme given in (5.7) is solved for the case for $\Delta = 0.5$ under the *high snr assumption* with $D(x)$ approximated by $\log(x)$. The next theorem gives us the power allocation profile at the different nodes for different values of $\kappa_i^2 := |h_{ai}|^2/|h_{bi}|^2$. An example power allocation profile is shown in Fig. 24.

Theorem F.2. *For finite L with $\Delta = 0.5$ and under the high snr approximation, the optimal power allocation for our proposed for different ranges of $\kappa_i^2 := |h_{ai}|^2/|h_{bi}|^2$ is given by,*

Case 1 $0 < \kappa_i^2 <= 1$,

$$P_{ai} = P\frac{2}{2+\kappa_i^2} \quad P_{bi} = P\frac{2\kappa_i^2}{2+\kappa_i^2} \quad P_{ri} = P\frac{2}{2+\kappa_i^2}$$

Case 2 $\kappa_i^2 > 1$,

$$P_{ai} = P\frac{2}{1+2\kappa_i^2} \quad P_{bi} = P\frac{2\kappa_i^2}{1+2\kappa_i^2} \quad P_{ri} = P\frac{2\kappa_i^2}{1+2\kappa_i^2}$$

Proof. The problem can be solved analytically using the method of Lagrange multipliers and using the Karush-Kuhn Tucker conditions following along the same lines as in the proof of theorem 1. □

3. Comparison

Theorem F.3. *For general L with $\Delta = 0.5$, the achievable rate using the channel inversion scheme with lattice decoding suffers at most a constant $\eta = 0.08972$ bits per complex channel use from the upper bound at high snrs, i.e.,* $\lim_{\mathsf{snr}\to\infty} \delta(\mathsf{snr}) \leq \eta$.

Proof. We first consider the optimization problem (5.1). For a given $\mathsf{snr} = P$ and

$\gamma \in \{a, b, r\}$, let $P_{\gamma i}(\mathsf{snr})$ be the optimal power allocation profile at the nodes in each of the i^{th} coherence time interval. We first establish that for the optimal power allocation profile for a given snr, $\lim_{\mathsf{snr}\to\infty} P_{\gamma i}(\mathsf{snr}) = \infty$, for every $\gamma \in \{a, b, r\}$ and $i \in \{1, 2 \ldots L\}$.

Let us assume that the above claim is not true. Then for the optimal solution, there is at least one $P_{\gamma i}(\mathsf{snr})$ and a constant M, such that $P_{\gamma i}(\mathsf{snr}) < M$ for all snr. Also for $\beta \in \{a, b, r\}$ and $j \in \{1, 2, 3 \ldots L\}$, let there be at least a $P_{\beta j}(\mathsf{snr})$ such that $\lim_{\mathsf{snr}\to\infty} P_{\beta j}(\mathsf{snr}) = \infty$, where either $\beta \neq \gamma$ or $j \neq i$.

Without loss of generality, let us assume that for the optimal solution $P_{ai}(\mathsf{snr}) < M$ for all snr, $\lim_{\mathsf{snr}\to\infty} P_{aj}(\mathsf{snr}) = \infty$ and $i \neq j$. Let us consider the terms in the objective function in (5.1) which are dependent on P_{ai} and P_{aj} for a given i and j. The dependent terms without the constant $\frac{1}{L}$ and $\Delta = 0.5$ can be expressed as

$$\begin{aligned} T_{aij}(\mathsf{snr}) = & \min\{C(|h_{ai}|^2 P_{ai}(\mathsf{snr})), C(|h_{bi}|^2 P_{ri}(\mathsf{snr}))\} \\ & + \min\{C(|h_{aj}|^2 P_{aj}(\mathsf{snr})), C(|h_{bj}|^2 P_{rj}(\mathsf{snr}))\}, \end{aligned}$$

where $C(x)$ is defined as $\log(1+x)$. Let us now choose the following readjusted power profile given below.

$$P^*_{ai}(\mathsf{snr}) = P_{ai}(\mathsf{snr}) + \frac{1}{4} P_{aj}(\mathsf{snr}).$$

$$P^*_{ri}(\mathsf{snr}) = P_{ri}(\mathsf{snr}) + \frac{1}{4} P_{aj}(\mathsf{snr}).$$

$$P^*_{aj}(\mathsf{snr}) = \frac{1}{4} P_{aj}(\mathsf{snr}).$$

$$P^*_{rj}(\mathsf{snr}) = P_{rj}(\mathsf{snr}) + \frac{1}{4} P_{aj}(\mathsf{snr}).$$

The readjusted power profiles do not violate the sum power constraint over all the nodes. Next, $T^*_{aij}(\mathsf{snr})$ formed by the readjusted power profile given by,

$$\begin{aligned} T^*_{aij}(\mathsf{snr}) = & \min\{C(|h_{ai}|^2 P^*_{ai}(\mathsf{snr})), C(|h_{bi}|^2 P^*_{ri}(\mathsf{snr}))\} \\ & + \min\{C(|h_{aj}|^2 P^*_{aj}(\mathsf{snr})), C(|h_{bj}|^2 P^*_{rj}(\mathsf{snr}))\} \end{aligned}$$

can be seen to be strictly greater than $T_{aij}(\mathsf{snr})$ for large snr from the concavity of $C(x)$ as follows. The second term in $T^*_{aij}(\mathsf{snr})$ suffers only a constant loss at large snr compared to the second term of $T_{aij}(\mathsf{snr})$. However, the first term in $T^*_{aij}(\mathsf{snr})$ can be made arbitrarily large with large snr compared to the first term of $T_{aij}(\mathsf{snr})$ as by assumption, $P_{ai}(\mathsf{snr})$ is bounded by a constant M. Hence $T^*_{aij}(\mathsf{snr})$ can be shown to be strictly larger than $T_{aij}(\mathsf{snr})$ for large snr. Since the new power allocation improves the objective function without violating the sum power constraint over the nodes and $P^*_{ai}(\mathsf{snr})$ is strictly larger than M for large snr, the original assumption that for the optimal solution $P_{ai}(\mathsf{snr})$ is bounded is false and hence $\lim_{\mathsf{snr}\to\infty} P_{ai}(\mathsf{snr}) = \infty$.

If suppose there is no such $P_{\beta j}(\mathsf{snr})$ such that $\lim_{\mathsf{snr}\to\infty} P_{\beta j}(\mathsf{snr}) = \infty$, then it means that the powers in all the nodes are bounded. Clearly the value of the objective function can be improved by readjusting the powers, as the total available power to all the nodes is arbitrarily large. The above arguments can also be repeated for any given $P_{\gamma i}(\mathsf{snr})$ and $P_{\beta j}(\mathsf{snr})$ by following similar steps as discussed above. Iterating the above proof procedure for all the coherence time intervals and all the nodes, it can be shown that the powers in all the nodes in all the coherence time intervals can be made arbitrarily large with snr.

The same result can also be shown for the optimization problem (5.7) by repeating the above mentioned steps. Based on the above observation, we can easily establish an upper bound and lower bound for $\log(1 + x)$ for all $x > M$, as $\log(x) < \log(1+x) \leq \log(x)+\epsilon$, where $\epsilon = \log(1+1/M)$ which can be made small by increasing M. Hence each of the terms in the objective function $C(x), D(x)$ can be bounded above by $\log(x) + \epsilon'$ and below by $\log(x)$, where ϵ' is a constant dependent on M and the finite channel gains between the nodes and the relay. Hence the power allocation profiles for the upper bound and the lower bound must be the same and equal to that obtained by using the *high snr approximation*. We therefore compare analytically the results of Theorem F.1 and Theorem F.2 under the *high snr approximation*. For different values of κ_i by comparison of the exchange rates, it can be easily show analytically that the channel inversion scheme suffers at most 0.08972 bits per complex channel use from the upper bound.

Hence for a snr reasonably large, it can be shown that $\delta(\mathsf{snr}) \leq 0.08972 + \epsilon$. The ϵ is a function of M and the finite channel gains between the nodes and the relays, and can be made arbitrarily small with increasing M and snr. Hence effectively it can be shown that at high SNRs, the gap between the upper bound and the achievable scheme is at most 0.08972 bits per complex channel use. $\square$

Theorem F.3, hence captures the loss due to adding the additional constraints to the upper bound, and the loss is found to be really small.

Practical issues with power allocation design: In the previous sections, we discussed techniques to compute the optimal power allocation for a given $\mathbf{h_a}, \mathbf{h_b}$ and $\mathbf{h_r}$. However, in practice we are interested in maximizing the average exchange capacity, i.e., the problem is to

$$\begin{aligned} \text{maximize} \quad & \mathbb{E}_{h_a,h_b}\big[\min\{\Delta C(|h_a|^2 P_a), (1-\Delta)C(|h_b|^2 P_r)\} \\ & + \min\{\Delta C(|h_b|^2 P_b), (1-\Delta)C(|h_a|^2 P_r)\}\big] \\ \text{subject to} \quad & \mathbb{E}_{h_a,h_b}\left[\Delta P_a + \Delta P_b + (1-\Delta)P_r\right] \leq P \\ & P_a, P_b, P_r \geq 0. \end{aligned}$$

Due to the ergodic nature of the channel, the above optimization problem is identical to (5.1) when $L \to \infty$. The result in Fig. 22 have been obtained by solving the optimization problem for one realization of $\mathbf{h_a}, \mathbf{h_b}$ and $\mathbf{h_r}$ but with $L = 100$. Note that while computing the optimal power allocation policy requires us to use a large value of L and optimize the policy, once this policy is fixed, the actual transmit power is chosen based only on the instantaneous channel realization.

G. Symmetric multi-hop case

1. Description

Here we are interested in exchanging information between two nodes through k relay nodes as shown in Fig.25. Here the channel gains are assumed to be symmetric. We can again show that rate of $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right)$ is achievable using structured coding even in this multiple hop scenario. It should be noted that the advantage of this scheme over the amplify and forward scheme [33] becomes more pronounced in the multi-hop case, since at each stage for the amplify and forward scheme, the channel noise is amplified and hence the amplify and forward scheme will suffer a huge rate loss as the number of hops increase. The problem model is shown in Fig. 25. The relay nodes and the nodes A and B can transmit only to the two nearest nodes. During a single transmission slot (n uses of the channel), a node can either listen or transmit. That is, it can not do both simultaneously. We explain our structured coding scheme using a simple example of a 3-relay network. The different transmissions are shown in the table given below.

Here node A and node B have data that need to be exchanged between each other. Each node has a stream of packets. Node A has packets named $\mathbf{u}_{A,1}, \mathbf{u}_{A,2}, \ldots$ and node B has packets named $\mathbf{u}_{B,1}, \mathbf{u}_{B,2}, \ldots$. In the first transmission slot the nodes

A and B transmit. Nodes A, B transmit vectors $\mathbf{x}_{A,1}$ and $\mathbf{x}_{B,1}$, respectively using our proposed lattice coding scheme. At the beginning of transmission, the node R_2 has no data to transmit in the first transmission slot, and hence it remains silent. The node R_1 and R_3 decode to $\mathbf{x}_{1,1} \mod \Lambda$ and $\mathbf{x}_{2,1} \mod \Lambda$, respectively. During the second transmission slot the nodes R_1 and R_3 transmit, while the other nodes remain silent. So, in each stage the nodes transmit and the listening nodes decode to a lattice point in the fine lattice in the Voronoi region of the coarse lattice. In every second transmission slot a new packet is transmitted to the relay nodes by the nodes A and B as can be seen from Table I. During slots $2, 4, 6$ nodes A, B transmits new packets into the relay channel. From this example, we can see that at the 4th slot the node A and B decode $\mathbf{x}_{B,1}$ and $\mathbf{x}_{1,2}$ respectively. This is because the node A receives $(\mathbf{x}_{1,1} + \mathbf{x}_{1,2} + \mathbf{x}_{2,1}) \mod \Lambda$ during the 4th transmission and, hence, since $\mathbf{x}_{1,1}, \mathbf{x}_{1,2}$ are already known at the node A, the node A can decode to $\mathbf{x}_{2,1}$ using modulo operation. The same argument holds for node B. From every two transmissions from this stage a new packet can be decoded at each node. This shows that for sufficiently large number packets we can achieve the rate of $\frac{1}{2}\log(\frac{1}{2} + \frac{P}{\sigma^2})$. A similar encoding scheme can be used for $L = 2$ nodes also, in the first slot, node A and R_2 transmit, while the others listen. In the next slot R_1 and node B transmit while the others listen and decode. Again the same rate of $\frac{1}{2}\log(\frac{1}{2} + \frac{P}{\sigma^2})$ is achievable.

2. Achievable rate

Theorem G.1. *For the multi hop scenario defined with L hops, an exchange rate of* $\frac{1}{2}\log(\frac{1}{2} + \frac{P}{\sigma^2})$ *is achievable with nested lattice encoding and decoding.*

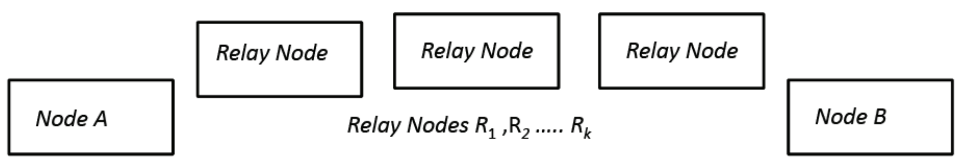

Fig. 25. Problem model for multi hop.

Table I. Table showing sequence of packets in the multi-hop case

Slot	Node A	Node R_1 (mod Λ)	Node R_2 (mod Λ)	Node R_3 (mod Λ)	Node B
1	Transmits $\mathbf{x}_{1,1}$	$\mathbf{x}_{1,1}$	Transmits	$\mathbf{x}_{2,1}$	Transmits $\mathbf{x}_{2,1}$
2	Remains Silent	Transmits	$\mathbf{x}_{1,1} + \mathbf{x}_{2,1}$	Transmits	Remains Silent
3	Transmits $\mathbf{x}_{1,2}$	$\mathbf{x}_{1,2} + \mathbf{x}_{1,1} + \mathbf{x}_{2,1}$	Transmits	$\mathbf{x}_{1,1} + \mathbf{x}_{2,1} + \mathbf{x}_{2,2}$	Transmits $\mathbf{x}_{2,2}$
4	Decodes $\mathbf{x}_{2,1}$	Transmits	$2(\mathbf{x}_{1,1} + \mathbf{x}_{2,1}) + \mathbf{x}_{1,2} + \mathbf{x}_{2,2}$	Transmits	Decodes $\mathbf{x}_{1,1}$
5	Transmits $\mathbf{x}_{1,3}$	$2(\mathbf{x}_{1,1} + \mathbf{x}_{2,1}) + \mathbf{x}_{1,2} + \mathbf{x}_{2,2} + \mathbf{x}_{1,3}$	Transmits	$2(\mathbf{x}_{1,1} + \mathbf{x}_{2,1}) + \mathbf{x}_{1,2} + \mathbf{x}_{2,2} + \mathbf{x}_{2,3}$	Transmits $\mathbf{x}_{2,3}$
6	Decodes $\mathbf{x}_{2,2}$	Transmits	$4(\mathbf{x}_{1,1}+\mathbf{x}_{2,1})+2(\mathbf{x}_{1,2}+\mathbf{x}_{2,2}) + \mathbf{x}_{1,3} + \mathbf{x}_{2,3}$	Transmits	Decodes $\mathbf{x}_{1,2}$

Proof. We can easily prove that the theorem holds for a general case L relay nodes in between. In our coding scheme in every two slots a new packet is sent out from the nodes A and B. After an initial $2L$ transmission slot delay, in every two slots the relay nodes receives a new packet from the other nodes. Here, we mean that for every two slots the relay node decodes to a lattice point which is a linear function of a new packet. Hence, at the decoding stage at the nodes B and A, we can decode after every two slots, since only one variable is unknown and only one new packet (or function of new packet) moves from one node to the other. Hence, we can still achieve the rate of $\frac{1}{2}\log(\frac{1}{2}+\frac{P}{\sigma^2})$. Moreover, the functions in each stage are bounded for a finite L and, hence, we can always perform the decoding at the receiver nodes. □

H. Concluding remarks

In this chapter we studied the bi-directional relay problem in which the channels between the nodes and the relays were assumed to have complex inputs with complex fading coefficients. We studied power allocation policies at the nodes for a two phase transmission scheme under the sum transmit power constraint over all nodes. For $\Delta = 0.5$, where each phase uses the channel exactly half the time, we obtained an upper bound on the exchange capacity as a solution to a convex optimization problem.

We proposed a scheme using nested lattice encoding with the transmit power chosen to be inversely proportional to the channel gains. This scheme has a reduced complexity compared to using a nested lattice with asymmetric rates. We obtained analytical solutions for the exchange capacity under the *high snr approximation* and showed that our proposed scheme can obtain a rate which is at most 0.09 bits away from the upper bound. For $\Delta \neq 0.5$ and individual power constraints for the nodes, the performance using a simple channel inversion power allocation policy differs significantly depending on the exact situation in hand. However, it can be shown that by using lattice codes with asymmetric rates [42] at the nodes, the upper bound can be achieved at high snrs. We also briefly looked at the extension to multiple hops and showed that for the symmetric case the upper bound can be achieved at high SNRs.

CHAPTER VI

CONCLUSION AND FUTURE WORK

To conclude, in this dissertation we studied several scenarios where joint coding schemes provide significant gains over separate coding schemes. We introduced several joint source channel coding schemes which are shown to be more robust to channel SNR variations. We also introduced joint network coding and physical layer coding schemes, that are shown to increase the throughput for bi-directional relaying. The problems considered in this dissertation, can be treated as a building block towards many interesting problems. Hence, we would like to conclude this dissertation by pointing towards some future lines of work.

1. In this dissertation, we have analyzed the HDA wyner-ziv and HDA costa for Gaussian sources. We also have a general model for relating the random variables using an auxiliary random variable. A possible future work is to find the distribution for the auxiliary random variable for some other sources, like the binary source with erasure side information. Though we presented an achievable scheme for the Gaussian case, a possible future work is developing a converse for the case of SNR mismatch.

2. The HDA costa scheme can be obtained by using both a random code construction as well as using a structured lattice code construction as in [10]. Both have the same performance in terms of distortion. A possible future work is to investigate, if there is a difference in the error exponents between the lattice code and the random code.

3. For the JSCC scheme for cognitive transmission and also for the case of the presence of an eavesdropper, we have studied the bandwidth matched case. It

would be an interesting problem to propose JSCC schemes for the bandwidth mismatched case.

4. We studied exchanging information using a bi-directional relay. An extension would be to study exchanging information over a diamond network, that has two intermediate relays than a single relay. Also there is a lot of recent work on using lattices for multi-cast in a wireless network using the deterministic approach [57]. It would be interesting to study similar techniques for exchanging information through a wireless network.

5. Another possible work is to study exchanging information over a fading channel, but with multi-hop. It would be interesting to see, if we can get results close to the upper bound for the multi-hop fading case also.

6. In our analysis of the bi-directional relay, we have made some ideal assumptions like perfect knowledge of channel state information (CSI). This implies that we can establish perfect time synchronization and phase synchronization. However it is not clear if these results are robust against lack of CSI. It would be interesting problem to obtain robust schemes for the case of imperfect CSI.

REFERENCES

[1] John G. Proakis, *Digital Communications*. New York: McGraw-Hill, 2000.

[2] C. E. Shannon, "A mathematical theory of communication ," *Bell Syst. Tech. J*, vol. 27, pp. 379–423, 623–656, 1948.

[3] S. Zhang, S. C. Liew, and P. P. Lam, " Physical-layer network coding," in *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking*. ACM, 2006, p. 365.

[4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *IEEE/ACM Transactions on Networking (TON)*, vol. 16, no. 3, pp. 497–510, 2008.

[5] U. Mittal and N. Phamdo, "Hybrid digital-analog (HDA) joint source-channel codes for broadcasting and robust communications," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1082–1102, 2002.

[6] C.E. Shannon, "Communication in the presence of noise," *Proc. of the IRE*, vol. 37, pp. 10–21, 1949.

[7] T. Goblick Jr, "Theoretical limitations on the transmission of data from analog sources," *IEEE Trans. Inf. Theory*, vol. 11, no. 4, pp. 558–567, 1965.

[8] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: Lossy source-channel communication revisited," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1147–1158, 2003.

[9] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[10] Y. Kochman and R. Zamir, "Analog matching of colored sources to colored channels," in *IEEE International Symposium on Information Theory*, 2006, pp. 1539–1543.

[11] S. Bross, A. Lapidoth, and S. Tinguely, "Superimposed coded and uncoded transmissions of a gaussian source over the gaussian channel," in *IEEE International Symposium on Information Theory*, 2006, pp. 2153–2155.

[12] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, Inc., 1968.

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

[14] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976.

[15] Z. Reznic, M. Feder, and R. Zamir, "Distortion bounds for broadcasting with bandwidth expansion," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3778–3788, 2006.

[16] N. Merhav and S. Shamai, "On joint source-channel coding for the Wyner-Ziv source and the Gel'fand-Pinsker channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2844–2855, 2003.

[17] A. Sutivong, M. Chiang, T. M. Cover, and Y. H. Kim, "Channel capacity and state estimation for state-dependent Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1486–1495, 2005.

[18] M. Tomlinson, “New automatic equaliser employing modulo arithmetic,” *Electronics Letters*, vol. 7(5/6), pp. 138, 1971.

[19] H. Harashima and H. Miyakawa, “Matched-transmission technique for channels with intersymbol interference,” *IEEE Trans. Commun.*, vol. 20, no. 4, pp. 774–780, 1972.

[20] S. I. Gel’Fand and M. S. Pinsker, “Coding for channel with random parameters,” *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[21] D. Slepian and J. Wolf, “Noiseless coding of correlated information sources,” *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[22] G. Kramer, “Topics in multi-user information theory,” *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 4-5, pp. 265–444, 2007.

[23] T. Berger, “Multiterminal source coding,” in *The InformationTheory Approach to Communications(CISM Courses and Lecture Notes)*, 1978, pp. 171–231.

[24] V. M. Prabhakaran, R. Puri, and K. Ramachandran, “Hybrid analog-digital strategies for source-channel broadcast,” in *43rd Allerton Conference on Communication, Control and Computing*, Allerton, IL, 2005.

[25] K. Narayanan, G. Caire, and M. Wilson, “Duality between broadcasting with bandwidth expansion and bandwidth compression,” in *IEEE International Symposium on Information Theory*, 2007, pp. 1161–1165.

[26] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[27] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[28] H. Yamamoto, “Rate-distortion theory for the Shannon cipher system,” *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, 1997.

[29] Federal Communications Commision. Cognitive radio technologies proceeding(CRTP). *ET Docket No. 03-108.* [Online]http://www.ctan.org/tex-archive/biblio/bibtex/contrib/doc/

[30] Federal Communications Commission Spectrum Policy Task Force, “Report of the spectrum efficiency working group,” Tech. Rep., FCC, Nov. 2002.

[31] A. Jovicic and P. Viswanath, “Cognitive radio: An information-theoretic perspective,” *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3945–3958, 2009.

[32] P. Larsson, N. Johansson, and K. E. Sunell, “Coded bi-directional relaying,” in *IEEE 63rd Vehicular Technology Conference*, Melbourne, Australia, May. 2006, pp. 851–855.

[33] S. Katti, S. Gollakota, and D. Katabi, “Embracing wireless interference: analog network coding,” in *SIGCOMM’07: Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications; Kyoto*, 2007, pp. 397–408.

[34] Y. Wu, P.A. Chou, and S.Y. Kung, “Information exchange in wireless networks with network coding and physical-layer broadcast,” in *Proc. of the 2005 Conference on Information Sciences and Systems*, Baltimore, Maryland, Mar. 16–18, 2005.

[35] T. J. Oechtering, C. Schnurr, I. Bjelakovic, and H. Boche, “Broadcast capacity region of two-phase bidirectional relaying,” *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, 2008.

[36] P. Popovski and H. Yomo, “Physical network coding in two-way wireless relay channels,” in *IEEE International Conference on Communications, ICC’07*, 2007, pp. 707–712.

[37] F. Xue and S. Sandhu, “PHY-layer network coding for broadcast channel with side information,” in *IEEE Information Theory Workshop, ITW’07*, 2007, pp. 108–113.

[38] Z. Shengli, S. C. Liew, and P. P. K. Lam. Physical layer network coding. [Online]http://arxiv.org/abs/0704.2475v1

[39] B. Nazer and M. Gastpar, “Lattice coding increases multicast rates for Gaussian multiple-access networks,” in *45th Annual Allerton Conference on Communication, Control and Computing*, Allerton, IL, Sept. 2007.

[40] K. Narayanan, M. P. Wilson, and A. Sprintson, “Joint physical layer coding and network coding for bi-directional relaying,” in *45th Annual Allerton Conference on Communication, Control and Computing*, Allerton, IL, Sept. 2007.

[41] S. J. Kim, N. Devroye, P. Mitran, and V. Tarokh. Achievable rate regions for bi-directional relaying. [Online]http://arxiv.org/abs/0808.0954v1

[42] W. Nam, S. Y. Chung, and Y. H. Lee, “Capacity bounds for two-way relay channels,” in *2008 IEEE International Zurich Seminar on Communications*, March 2008, pp. 144–147.

[43] J. Körner and K. Marton, “How to encode the modulo-two sum of binary sources (Corresp.),” *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, 1979.

[44] B. Nazer and M. Gastpar, “Computation over multiple-access channels,” *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3498–3516, 2007.

[45] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *European Transactions on Telecommunications*, vol. 19, no. 4, pp. 455–474, 2008.

[46] U. Erez and R. Zamir, "Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.

[47] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.

[48] R. De Buda, "Some optimal codes have structure," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 6, pp. 893–899, 1989.

[49] T. Linder, C. Schlegal, and K. Zeger, "Corrected proof of de Buda's theorem [lattice channel codes]," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1735–1737, 1993.

[50] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 273–278, Jan 1998.

[51] G. D. Forney Jr., "On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener," in *41st Annual Allerton Conference on Communication, Control and Computing*, Oct. 2003, pp. 430–439.

[52] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 409–417, 1994.

[53] C. E. Shannon, “Probability of error for optimal codes in a Gaussian channel,” *Bell Syst. Tech. J*, vol. 38, no. 3, pp. 611–656, 1959.

[54] E. Hlawka, J. Schoissengeier, and R. Taschner, *Geometric and Analytic Number Theory*. Berlin/NY: Springer-Verlag, 1991.

[55] I. J. Baik and S. Y. Chung, “Network coding for two-way relay channels using lattices,” in *2008 IEEE International Conference on Communications - ICC ’08*, May 2008, pp. 3898–3902.

[56] Y. Wu, “Broadcasting when receivers know some messages a priori,” in *IEEE International Symposium on Information Theory*, 2007, pp. 1141–1145.

[57] W. Nam and S. Y. Chung, “Relay networks with orthogonal components,” in *Proc. 46th Annual Allerton Conference*, Allerton, IL, 2008, pp. 738–745.

VITA

Makesh Pravin John Wilson obtained a B.E. degree in Electronics and Communication Engineering from College of Engineering - Guindy (Anna University), Chennai in May 2004. He also obtained a Ph.D. degree in Electrical and Computer Engineering from Texas A&M University, College Station, TX - 77845 in May 2010. He can be reached at Qualcomm Inc., 5775 Morehouse Drive, San Diego, CA - 92121 or at mjohnwil@qualcomm.com