TÉCNICO LISBOA

Distributed Source Coding Based on Integer-Forcing

Pedro Jorge Martins Teixeira

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. João Manuel de Freitas Xavier
Prof. Francisco António Taveira Branco Nunes Monteiro

Examination Committee

Chairperson: Prof. José Eduardo Charters Ribeiro da Cunha Sanguino
Supervisor: Prof. Francisco António Taveira Branco Nunes Monteiro
Member of the Committee: Prof. Mário Alexandre Teles de Figueiredo

June 2018

To my parents

Declaration

I declare that this document is an original work of my own authorship and that if fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

I would like to express my feeling of gratitude towards my supervisors Professor Francisco Monteiro and Professor João Xavier for giving me the chance to write this thesis. Individually, a special appreciation to Professor Francisco Monteiro for the constant guidance throughout these months, for always being available to help in spite of a busy academic life, and for the contagious motivation to do scientific research. Towards Professor João Xavier I would like to express my admiration for his expertise without which many parts of this thesis would not be possible. Additionally, I would also like to thank Professor Juan Acebrón for providing access to the computers *Tsunami* (at ISCTE-IUL) and *Science* (at INESC) to perform the necessary computationally intensive simulations.

On a personal level, a special thanks to all my friends for the unconditional support during this period of my life, and to my girlfriend Margarida Simão for being right beside me since day one.

Last but not least, I want to express my deepest gratitude to my family, specially to my parents Dora and Jorge, I owe them everything.

Resumo

Uma das áreas em comunicações com um desenvolvimento significativo nos últimos anos é a área relativa à codificação distribuída de fonte. A ideia principal que suporta este esquema de compressão é a de explorar a correlação espacial existente entre as observações de codificadores não cooperantes. A codificação de fonte com *forçagem-a-inteiros* é um caso específico de codificação distribuída de fonte com perdas em que todos os codificadores utilizam o mesmo *reticulado aninhado* para codificar as observações e de seguida enviar essa informação individualmente para um descodificador. Este descodificador aplica um conjunto de combinações lineares com coeficientes inteiros entre os sinais recebidos para mais tarde as inverter de modo a obter as estimativas finais das observações com uma certa distorção associada. Este esquema de compressão é explicado em detalhe nesta tese, assim como o problema de optimização subjacente de encontrar os coeficientes inteiros mais apropriados para executar as combinações lineares. Numa primeira abordagem, este problema é resolvido com recurso ao algoritmo LLL para redução *modulo-reticulado* que apenas encontra uma solução aproximada, e portanto, de modo a encontrar a solução exacta, é utilizado nesta tese um algoritmo baseado no problema dos *sucessivos mínimos*. O esquema é ainda aplicado a um cenário onde existe um conjunto de possíveis modelos de correlação e incerteza associada relativamente a qual destes modelos é o mais indicado para descrever a correlação num dado instante temporal. Para finalizar, é analisada uma versão de baixa complexidade deste esquema que envolve um custo relativamente ao desempenho obtido. Todo o trabalho aqui apresentado é suportado por ilustrações adequadas e resultados de simulações da teoria apresentada.

Palavras-chave: Codificação distribuída de fonte com perdas, codificação de fonte com *forçagem-a-inteiros*, correlação espacial, *reticulados aninhados*, redução *modulo-reticulado*, problema dos *sucessivos mínimos*.

Abstract

One of the research areas in communications with significant development in recent years is distributed source coding (DSC). The main idea behind DSC is to exploit the existing spatial correlation among the observations of non-cooperating encoders. Integer-forcing source coding (IFSC) is a specific case of lossy DSC, in which all encoders employ the same nested lattice codebook to code their observations and send them individually to the decoder, which instead of directly retrieving the individual signals, first recovers a set of integer linear combinations of those signals and then inverts it to obtain the final estimates within some predefined distortion measure. A comprehensive study of this scheme is provided in this thesis, which also addresses the underlying optimization problem of finding the appropriate integer coefficients to perform the integer linear combinations. As a first approach, this problem is solved with the LLL lattice reduction algorithm, which at best, yields an approximate solution, and so, an alternative algorithm that returns the exact solution based on the successive minima problem (SMP) is also explored. Further, the IFSC scheme is applied to a situation where the correlation among the sources belongs to a finite set of possible correlation models, each of which with a given known probability. Finally, a simpler version of IFSC is analysed in order to allow an easier implementation at the cost of performance degradation. All the work herein presented is supported by appropriate illustrations and simulation results in the form of rate-distortion curves.

Keywords: Lossy distributed source coding, integer-forcing source coding, spatial correlation, nested lattices, modulo-lattice reduction, successive minima problem.

Contents

List of Tables

List of Figures

Nomenclature

Scalars, Vectors and Matrices

x	Scalar x.
$\mathbf{x}$	Vector $\mathbf{x}$.
x_i	Entry i of vector $\mathbf{x}$.
$\mathbf{x}_{i:j}$	Subvector formed by the entries $i, i+1, ..., j$ of $\mathbf{x}$.
$\mathbf{x} \setminus \{0\}$	Non-zero vector $\mathbf{x}$.
$\langle \mathbf{x}, \mathbf{y} \rangle$	Inner product between vectors $\mathbf{x}$ and $\mathbf{y}$.
$\| \mathbf{x} \|_1$	1-norm of vector $\mathbf{x}$.
$\| \mathbf{x} \|_\infty$	Inf-norm of vector $\mathbf{x}$.
$\mathbf{X}$	Matrix $\mathbf{X}$.
$x_{i,j}$	Entry in the i^{th} line and j^{th} column of matrix $\mathbf{X}$.
$\det(\mathbf{X})$	Determinant of matrix $\mathbf{X}$.
$\mathbf{X}_{[\setminus j]}$	Submatrix formed by all columns of $\mathbf{X}$ with the exception of the j^{th} column.
$\mathbf{I}$	Identity matrix.
$\mathbf{K}_{\mathbf{xx}}$	Covariance matrix.
$\mathbf{T}$	Unimodular matrix.
$\mathbf{G}$	Gram matrix / Lattice generator matrix.
$\mathbf{Q}$	Orthogonal matrix.

Operators and Sets

$\mathbb{E}[\cdot]$	Expected value operator.
$P(x)$	Probability of x.
$\mathcal{N}(\mu, \sigma^2)$	Normal distribution with mean value μ and variance σ^2.
$\mathbb{Z}$	Set of integer numbers.
$\mathbb{R}$	Set of real numbers.
$\mathcal{O}(\cdot)$	Complexity order, big O notation.
$\ln(x)$	Base-e logarithm of x.
$\log_2(x)$	Base-2 logarithm of x.
$\log_{10}(x)$	Base-10 logarithm of x.
$\mathrm{sgn}(x)$	Signal function.
$\mathrm{rect}(x)$	Rectangular function.

$\exp(x)$ Exponential function.

$\lceil \cdot \rfloor$ Rounding to the closest integer.

$\lceil \cdot \rceil$ Ceiling function.

$\lfloor \cdot \rfloor$ Floor function.

$|\cdot|$ Absolute value.

$\mathcal{Q}(\cdot)$ Quantizer to the nearest neighbour.

$\mathsf{Q}(\cdot)$ Q-function.

Superscripts

$\mathbf{X}^T$ Transpose of a matrix $\mathbf{X}$.

$\mathbf{X}^{-1}$ Inverse of a matrix $\mathbf{X}$.

Lattice Theory

Λ Lattice.

$\Lambda(\mathbf{G})$ Lattice generated by the lattice generator matrix $\mathbf{G}$.

Λ_c Coarse lattice.

Λ_f Fine lattice.

λ Lattice point.

$[\cdot] \bmod \Lambda$ Modulo reduction to lattice Λ.

$\mathcal{Q}_\Lambda(\cdot)$ Quantization onto lattice Λ.

P_λ Partition cell of a lattice point λ.

$\mathcal{V}$ Voronoi region.

$\mathsf{Vol}(\mathcal{V})$ Volume of the Voronoi region.

$r_{eff}(\Lambda)$ Effective radius of lattice Λ.

$\sigma^2(\Lambda)$ Second moment of lattice Λ.

$\mathcal{C}$ Voronoi codebook.

θ_k kth successive minimum of a lattice.

$\mathbf{e}$ Quantization error vector.

$\mathbf{d}$ Random dither vector.

$\mathbf{u}$ Estimation error vector.

Integer-Forcing Source Coding

K Number of encoders.

n Numbertime realizations.

R Rate.

d Target distortion.

$\mathbf{x}_k$ Source vector of the kth encoder.

$\tilde{\mathbf{x}}_k$ Vector received by the decoder from the kth encoder.

$\hat{\mathbf{x}}_k$ Estimate of $\mathbf{x}_k$.

$\mathbf{u}_k$ Estimation error vector of the kth source vector.

$\mathbf{X}$ Matrix containing the K source vectors.

$\tilde{\mathbf{X}}$ Matrix containing the K vectors received by the decoder.

$\widehat{\mathbf{X}}$ Matrix containing the K estimation vectors.

$\mathbf{U}$ Matrix containing the K estimation error vectors.

$\mathbf{A}$ Integer-valued full-rank matrix $\mathbf{A}$.

$\mathbf{a}_k^T$ kth row of the matrix $\mathbf{A}$.

$\mathbf{a}_k$ Transpose of the kth row of the matrix $\mathbf{A}$.

$\mathbf{A}^*$ Optimal integer-valued full-rank matrix $\mathbf{A}$.

M Number of transmitters.

w_m Message of the mth transmitter.

$\mathbf{s}_m$ Signal transmitted by the mth transmitter over n channel uses.

$\mathbf{z}_k$ White Gaussian noise vector added at the kth encoder.

$\mathbf{S}$ Matrix containing the M signals transmitted.

$\mathbf{Z}$ Matrix containing the K noise vectors.

$\mathbf{H}$ Channel matrix.

SNR Signal-to-noise ratio.

R_{IFSC} Rate attained with the integer-forcing source coding scheme.

R_{BT} Rate attained with the Berger-Tung scheme.

R_{Naive} Rate attained with the naive scheme.

Information-Theoretic Rate-Distortion

β Hyper-ellipsoid constant.

$\mathbf{C}^*$ Optimal integer-valued full-rank matrix $\mathbf{C}$.

$\mathbf{F}$ Row echelon form reduced matrix.

$\mathbf{R}_{red}$ Reduced basis matrix.

$\mathbf{R}^T$ Lower triangular matrix.

$\mathbf{R}$ Upper triangular matrix.

Semi-Blind Correlation Model

δ Random variable that follows a Bernoulli distribution.

$\mathbf{A}_A^*$ Optimal integer-valued full-rank matrix $\mathbf{A}$ for the correlation model A.

$\mathbf{A}_{ext}^*$ Optimal integer-valued full-rank matrix $\mathbf{A}$ for the extended correlation model.

$\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}}$ Covariance matrix that describes correlation model A.

$\tilde{\mathbf{K}}_{\mathbf{xx}}$ Selected covariance matrix.

N Size of the set of possible covariance matrices.

$\mathbf{R}_A$ Lattice generator matrix for correlation model A.

$\mathbf{R}_{ext}$ Extended lattice generator matrix.

One-Shot Integer-Forcing Source Coding

q Quantization step.

n_q^2 Quantization noise power.

P_{ol} Probability of an overload event.

$\delta(P_{ol})$ Rate penalty for a given P_{ol}.

$\mathbf{b}_k^T$ kth row of the matrix $\mathbf{A}^{-1}$.

$\mathbf{b}_k$ Transpose of the kth row of the matrix $\mathbf{A}^{-1}$.

OL Binary random variable associated with the overload event.

$\mathcal{D}_{OL=1}$ Domain where $OL = 1$.

$\mathcal{D}_{OL=0}$ Domain where $OL = 0$.

$\hat{d}$ Distortion value smaller than d.

R_{OIFSC} Rate attained with the one-shot integer-forcing source coding scheme.

Glossary

5G	Fifth Generation of Mobile Networks
BS	Base Station
BT	Berger-Tung
CP	Central Processor
CVP	Closest Vector Problem
DSC	Distributed Source Coding
I.I.D.	Independent and Identically Distributed
IFSC	Integer-Forcing Source Coding
IF	Integer-Forcing
LLL	Lenstra–Lenstra–Lovász
LSBs	Least Significant Bits
MAC	Multiple Access Channel
MIMO	Multiple-Input Multiple-Output
MSBs	Most Significant Bits
MSE	Mean Square Error
MT	Multi-terminal
NP	Non-deterministic Polynomial-time
OIFSC	One-Shot Integer-Forcing Source Coding
OL	Overload
RAN	Radio Access Network
RSMP	Reduced Successive Minima Problem
SIVP	Shortest Independent Vector Problem
SMP	Successive Minima Problem
SM	Successive Minima
SNR	Signal-to-Noise Ratio
SVP	Shortest Vector Problem
SW	Slepian-Wolf
UE	User Equipment
WZC	Wyner-Ziv coding

Chapter 1

Introduction

This introduction begins with the motivation for this thesis, followed by a brief overview of the topic at hand and the groundwork that sustains the work here presented. To close this introduction, an outline of this dissertation is presented in the last section.

1.1 Motivation

In recent years, one of the research areas in communications with particular growth is the one involving wireless sensor networks. These networks are mainly constituted by several low-power and usually low-cost wireless sensors that are deployed for specific information gathering like temperature measurements, audio collection and video recording. In contrast to other network elements with enough computational power to sustain all sort of applications, these sensors must work under a set of constraints. One of these constraints lies on energy consumption, since in most applications the wireless sensor is expected to carry out its mission depending on a battery that is unlikely to be recharged. Another constraint has to do with the reduced complexity of said wireless sensors. These limitations have a significant impact on the wireless sensor network regarding the amount of information that the sensor node can collect and process, and the way it communicates with the other elements of the network. To address these limitations, one of the existing technologies is distributed source coding (DSC), that presents an effective source compression scheme based on the exploitation of the existing correlation between the information to be collected and transmitted. An overview of this compression scheme is presented in the following section.

1.2 Overview of Distributed Source Coding

1.2.1 Historical Overview

Distributed source coding, as the name indicates, is a particular case of source coding, which is a concept introduced by Claude Shannon in his 1948 famous paper [1]. His pioneering work brought to light

two types of source coding: lossless source coding, where the compressed data can be reconstructed either perfectly or with a probability of error approaching zero, and lossy source coding, in which greater efficiency in data representation is obtained through the tolerance of some level of inaccuracy or distortion in the resulting reproduction [2]. With respect to lossless source coding, Shannon's paper introduces the approach to deriving upper bounds on the rates needed to reliably describe a source and provides a proof that no better rates can be achieved. For lossy source coding, a description of the trade-off between rate and distortion is also provided in that work. Later, in a 1959 paper [3], Shannon revisits this trade-off providing more details of the proof and coining the term *rate distortion function* to describe that bound, which is of great importance throughout this dissertation. Since that work, there has been a lot of research in both lossless and lossy source coding.

Of particular interest to this dissertation was the development of multi-terminal (MT) source codes, which consist of data compression algorithms for networks with multiple transmitters of information, multiple receivers, or both [2]. In this context, it is impossible to bypass the work of Slepian and Wolf (SW) [4] on DSC networks, where source coded descriptions are sent by independent encoders to a single decoder. Slepian and Wolf theoretically showed in 1973 that separate encoding may be applied instead of joint encoding without any loss of compression efficiency as long as the correlation between sources is preserved throughout the transmission to the receiver, and that joint decoding is performed. After that, in 1976, Wyner and Ziv extended (in [5]) the SW problem to lossy source coding of Gaussian sources relying on side information to formulate the Wyner-Ziv coding (WZC) problem. These major contributions on the theoretical foundations of DSC were followed by other important contributions in both lossless DSC and lossy DSC, summarized in Tables 1.1 and 1.2.

Year	**Author(s)**	**Contribution**
1973	Slepian and Wolf [4]	Determined the maximum achievable compression rates, demonstrating that there is no loss of coding efficiency when comparing separate encoding with joint encoding as long as joint decoding is allowed.
1974	Cover [6]	Generalized the SW problem to more than two sources.
1980	Cover *et al.* [7]	Considered the multiple access channel (MAC) of the SW problem, demonstrating that designing the source and channel coding in a separate manner is not optimal.
2005	Cristescu *et al.* [8]	Solved the problem of supporting the communication of a large set of correlated sources with a set of destinations.
2006	Barros *et al.* [9]	Considered the problem of multicasting correlated sources to a single destination where a limited inter-user communication was allowed.
2015	Lu *et al.* [10]	The outage probability of a multiple access relay channel was derived for correlated sources assisted by relay-based transmission.

Table 1.1: Summary of the major contributions in lossless DSC, as presented in [11].

The research on DSC was born in the realms of information theory as mentioned but, recently, both communication theory and signal processing have also contributed to this research [11]. Furthermore, since DSC is proven to provide efficient solutions in scenarios where a source correlation exists, it

Year	Author(s)	Contribution
1976	Wyner and Ziv [5]	Extended the classic SW problem to lossy source coding relying on side information.
1977	Berger [12]	Introduced the MT coding problem for two physically separated sources.
1985	Heegard *et al.* [13]	Extended the MT problem of [12] to more than two users.
1996	Zamir [14]	Determined the rate loss when comparing the WZC scheme to the separate decoding scenario.
1997	Oohama [15]	Considered the direct MT problem for quadratic Gaussian sources.
2002	Zamir *et al.* [16]	Proposed the use of nested lattice codes in the WZC problem.
2008	Yang *et al.* [17]	Proposed SW coded quantization for the direct and indirect MT problem.
2014	Oohama [18]	Derived the inner and outer bound of the rate distortion region for the case of correlated sources.

Table 1.2: Summary of the major contributions in lossy DSC, as presented in [11].

has been applied not only in wireless sensor networks but also in a wide range of applications where exploring this correlation is advantageous. The relationship of DSC to its theoretical background and to its use in diverse applications is summarized in the diagram depicted in figure 1.1, based on the one presented in [11].

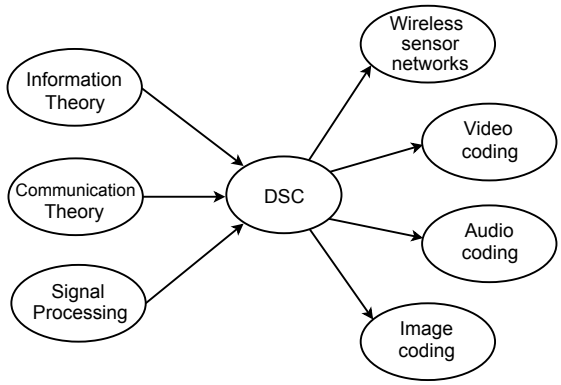


Figure 1.1: Relationship of DSC to its theoretical background and to its use in diverse applications.

1.2.2 Distributed Source Coding Principle

According to the definition provided in [11], DSC refers to the problem of compressing several physically separated but correlated sources, which are unable to communicate with each other, by exploiting that the receiver with enough processing power can perform joint decoding of the encoded signals. At a first glance, this source coding scheme may seem less powerful than the one with joint encoding and joint decoding. However, as mentioned earlier, due to the exploitation of the existing correlation between sources, the DSC scheme can in fact compete with its joint encoding and decoding counterpart [19], providing an appropriate solution to applications where joint encoding is not possible and it is preferable to have the computational burden on the receiver's side. With this in mind, the ultimate goal of the

DSC scheme is to explore the existing correlation between the sources at the encoder's side in order to minimize the transmission energy and processing power required by the encoders, which can be seen as, for example, sensors in a wireless sensor network, while maintaining reliable communication.

In order to provide some insight on the feasibility of the DSC to compress correlated sources, the following canonic example is presented, also available in [11] and an equivalent one in [38]. Consider the real-world application where the temperature measurements of two nearby locations are transmitted to a joint decoder at the central weather station as depicted in figure 1.2. To simplify this example without loss of generality, it is assumed that these two temperature measurements do not differ more than one temperature value from one another. First, both encoders group all the possible temperature readings, i.e., codewords, into disjoint sets or bins as represented in figure 1.3. If, for example, encoder Y transmits a reading $y = 8$ using a full representation, say 6 bits, then encoder X would only need to transmit the 2 bits indicating the specific bin its reading $x = 9$ belongs to. At the receiver's side, the joint decoder exploits the correlation between the pair of temperature readings by comparing the signal transmitted by encoder Y to each member of the particular bin represented by the specific 2 bit index sent by encoder X. By doing so, it finds that only the bin entry $x = 9$ is close enough to $y = 8$ to satisfy the existing correlation.

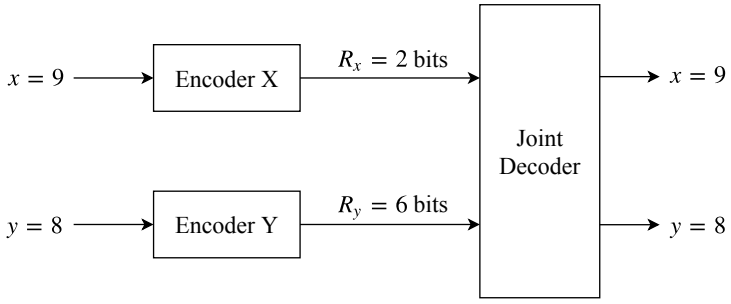


Figure 1.2: DSC example schematic.

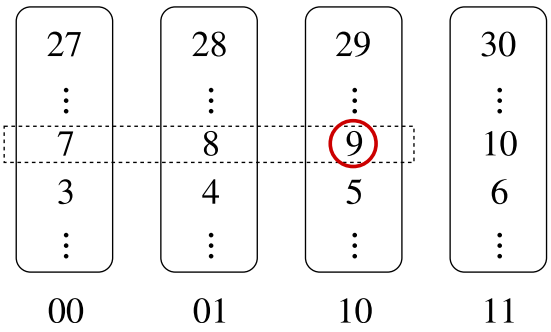


Figure 1.3: Disjoint bins used by the encoders in the first DSC example.

If encoder Y transmits a reading $y = 7$ with a 6 bits representation, and encoder X a reading $x = 6$ again with only 2 bits indicating the specific bin 6 belongs to, the decoder can once more decode encoder X's reading by exploiting the existing correlation. This case is illustrated in figure 1.4. Through this process a rate reduction of $6 - 2 = 4$ bits per sample can be attained.

The partition of all possible temperature readings, i.e., of all possible outcomes of the source, into

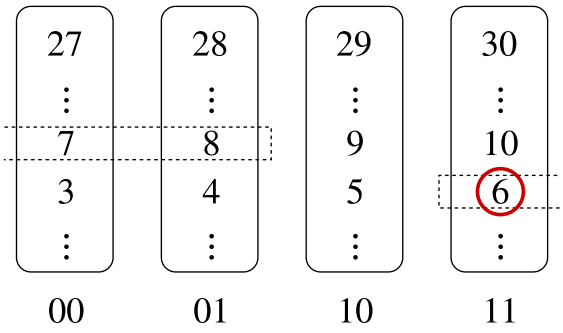


Figure 1.4: Disjoint bins used by the encoders in the second DSC example.

disjoint sets or bins in the previous example is referred to as a *binning process*[1]. Binning is a key concept in the DSC scheme and motivated researchers to propose various forms of codes for efficient binning in both lossless and lossy DSC. Error correcting codes also have a role in DSC [20, 30, 38], but that topic is outside of the scope of this thesis. One particular proposition was the aforementioned contribution made by Zamir *et al.* in [16], where the use of nested lattice codes is suggested to perform this binning process in a lossy DSC context.

1.3 Integer-Forcing

The concept of integer-forcing (IF) was first introduced for a new communication architecture based on IF linear receivers in [21]. In that work, a new type of linear receivers is presented for the Gaussian multiple-input multiple-output (MIMO) channel, based on the decoding of multiple integer linear combinations of the incoming symbols. Provided that the integer coefficients are chosen appropriately, these integer linear combinations can be solved for the original codewords. It has been proven in [21] that the IF-based receiver architecture achieves the diversity-multiplexing tradeoff [22] of uncoded MIMO spatial multiplexing. Further, it was proven in [23] that by using a precoded IF framework it is possible to achieve the capacity of any Gaussian MIMO channel up to a gap that depends only on the number of transmit antennas.

Given the benefits that the IF concept brought to MIMO detection, MIMO precoding, and to physical-layer network coding [28, 29], Ordentlich and Erez proposed in 2017 an IF-based framework for DSC [24]. That work proposes a novel framework for distributed lossy compression of correlated Gaussian sources under a minimum mean squared error distortion measure with the aid of nested lattice codes, dubbed integer-forcing source coding (IFSC). IFSC could potentially be used in the upcoming architecture of 5G cloud-RAN (radio access network) where different base stations (BS) play the role of the encoders and simultaneously listen to copies of the signal coming from one user equipment (UE), which are necessarily correlated [25]. This example is illustrated in figure 1.5, based on the proposal in [25].

The IFSC scheme constitutes the main groundwork of this thesis, whose outline is provided in the next section.

[1] An explanation of the binning process is provided by the section “Slepian-Wolf Coding Examples” in [20].

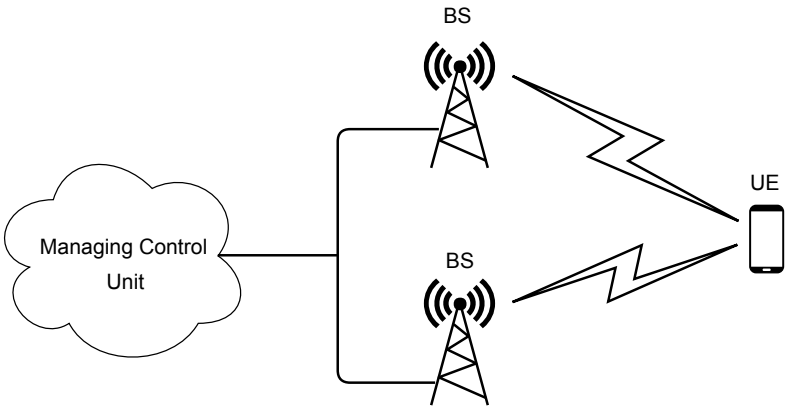


Figure 1.5: Cloud radio access network setup. Two BS, which play the role of encoders, compress and forward the correlated signals they receive from user equipments.

1.4 Thesis Outline

The starting point for the research presented in this work is a very recent framework for lossy DSC with the aid of nested lattice pairs. To fully understand the topic, knowledge from a variety of subjects is required as probability theory, lattice theory, and advanced matrix theory, among others. This thesis supplies the basic definitions and required notation to aid the understanding of the topic, referring to the appropriate bibliography whenever it is necessary. Furthermore, every chapter of this thesis provides a simulation of the discussed theory and proposed solutions. The necessary results are presented in the form of rate-distortion curves to act in conformity with the research community of information theory in the lossy DSC context.

The outline of this thesis in terms of chapters and respective contents is made as follows:

Chapter 2 - Lattice-Based Integer-Forcing Source Coding: In chapter 2 the lattice-based IFSC scheme is introduced, based on the work presented in [24]. Before a detailed explanation of the scheme is given, the necessary lattice theory is introduced since it lays the fundamentals not only to the formulation of the IFSC scheme, but also for the rest of this dissertation. Next, the IFSC scheme with nested lattice pairs is presented in a way that focus on "the geometry of lattice-based integer forcing" and how it takes advantage of the correlation between the observations of the encoders. The chapter establishes the underlying optimization problem that directly affects the performance of IFSC and that is here initially solved (as done in [24]) by means of the famous Lenstra–Lenstra–Lovász (LLL) algorithm for lattice basis reduction algorithm [26, 27]. In the final part of the chapter a replication of the results in the original proposal of IFSC [24] is made and analyzed.

Chapter 3 - Information-Theoretic Rate-Distortion of Integer-Forcing Source Coding: In this chapter a recently proposed alternative to solve the successive minima problem is applied to the underlying optimization problem of the IFSC scheme. This alternative algorithm is an *exact* algorithm that provides an optimal solution to this problem, and therefore a performance comparison is made

between its solutions and the ones obtained when using the LLL-based approximation.

Chapter 4 - Semi-Blind Correlation Model: In this chapter a solution to the problem of adapting the IFSC scheme to a scenario where there is a finite set of possible correlation models instead of only a fixed one is proposed. The formulation of this "extension of the problem" heavily relies on the lattice theory presented in chapter 2, and its evaluation is made for some basic setups by analyzing the obtained rate-distortion curves and comparing them with the pre-established benchmarks.

Chapter 5 - One-Shot Integer-Forcing Source Coding: After having analyzed the IFSC scheme based on nested pairs of high-dimensional non-orthogonal lattices, in this chapter the one-shot integer-forcing source coding scheme, based on a 1-dimensional nested lattice pair in each dimension, is analyzed. This simpler version of IFSC results from the possible trade-off between complexity and performance allowed by the original IFSC scheme. That performance degradation is assessed in terms of the rate-distortion curves obtained for some predefined correlation models.

Chapter 6 - Conclusions: In the last chapter, an overview of the main results and conclusions drawn from each chapter is summarized, and some extensions to this work are pointed out.

Chapter 2

Lattice-Based Integer-Forcing Source Coding

In this chapter, a comprehensive introduction to the IFSC scheme is given, and the theory supporting this state-of-the-art framework is presented. After that, a reproduction of the results currently available is presented to set the performance of this new approach and to serve as a benchmark for the remaining of this dissertation.

2.1 Introduction

The IFSC scheme is a new framework proposed by Ordentlich and Erez in [24] which is inspired by the pioneering work presented in [21] for MIMO detection, and brings some of its central ideas to the problem of source coding. In particular, this scheme tackles the problem of DSC that consists of multiple distributed non-cooperating encoders that have access to correlated observations of some phenomenon, and a final destination that has to decode all the individual observations. This problem arises in various scenarios as the one depicted in figure 2.1, where a few distributed temperature sensors are connected via finite rate links to a central processor, but not between them, and must describe their temperature readings to the central processor.

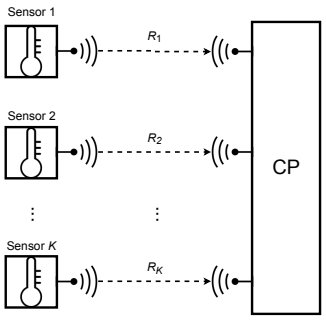


Figure 2.1: Distributed non-cooperating temperature sensors connected via finite rate links to a central processor (CP).

A special case of this problem is that of distributed lossy compression of jointly Gaussian random variables under a quadratic distortion measure. The setting considered here to describe this case has K encoders and one decoder, as represented in figure 2.2. As stated before, the K encoders are not allowed to cooperate and each one has access to a vector $\mathbf{x}_k \in \mathbb{R}^{1\times n}$ of n independent and identically distributed (i.i.d) realizations of the random variable x_k for $k = 1, ..., K$.

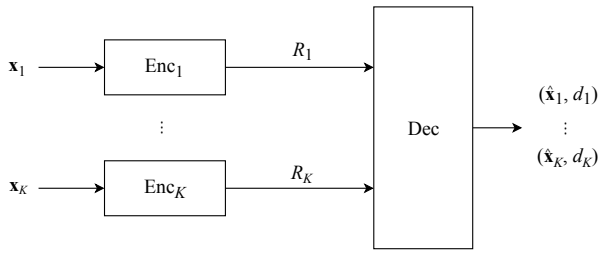


Figure 2.2: Distributed source coding setup.

The vector containing the set of these correlated random variables, $\mathbf{x} = [x_1 \cdots x_K]^T \in \mathbb{R}^{K\times 1}$, is assumed to be Gaussian with zero mean and its correlation is expressed by the covariance matrix given by

$$\mathbf{K_{xx}} \triangleq \mathbb{E}(\mathbf{x}\mathbf{x}^T). \tag{2.1}$$

The encoding process resorts to each encoder mapping its observation, vector $\mathbf{x}_k$, to an index using an encoding function

$$\mathcal{E}_k : \mathbb{R}^n \to \{1, ..., 2^{nR_k}\}.$$

From a general point of view, the encoding process is a mapping of each row of a $K\times n$ matrix to an entry of a column vector. Each row of that $K \times n$ matrix corresponds to a vector $\mathbf{x}_k$ and the corresponding entry of the column vector to its index:

$$\begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ & & \vdots & \\ x_{K1} & x_{K2} & \dots & x_{Kn} \end{bmatrix}_{K\times n} \xrightarrow{\mathcal{E}} \begin{bmatrix} \{1, ..., 2^{nR_1}\} \\ \vdots \\ \{1, ..., 2^{nR_K}\} \end{bmatrix}_{K\times 1}.$$

These indexes take values for each set of n observations of one encoder in each row in the set $\{1, ..., 2^{nR_k}\}$ and are sent to the decoder.

On the other terminal, the decoder has K decoding functions

$$\mathcal{D}_k : \{1, ..., 2^{nR_1}\} \times ... \times \{1, ..., 2^{nR_K}\} \to \mathbb{R}^n,$$

for $k = 1, ..., K$. When the decoder receives the K previously mentioned indexes, it generates estimates of each vector $\mathbf{x}_k$ given by

$$\hat{\mathbf{x}}_k = \mathcal{D}_k\big(\mathcal{E}_1(\mathbf{x}_1), ..., \mathcal{E}_K(\mathbf{x}_K)\big). \tag{2.2}$$

This type of DSC is lossy, in the sense that instead of perfect recovery, the decoder provides estimates

of the original source to within some target distortion d [30].

The lossy distributed source coding problem can be divided into the *symmetric* rate setup and into the *asymmetric* rate setup. Throughout this thesis, following the same setup of [24], only the former is considered where $R_1 = ... = R_K = R$, and $d_1 = ... = d_K = d$. This choice allows a simpler explanation of the IFSC scheme and makes the simulations easier to perform. Furthermore, this *symmetric* rate setup matches the requirements of various applications where the coding burden has to be equally distributed over the available encoders. Nevertheless, this setup can be generalised to the *asymmetric* case, as suggested in [24]. With this in mind, also using the same notation in [24], one has that a rate-distortion vector (R, d) with the necessary rate R to achieve the distortion d is achievable if, for n large enough, there exist encoding functions $\mathcal{E}_1, ..., \mathcal{E}_K$ and decoding functions $\mathcal{D}_1, ..., \mathcal{D}_K$ that satisfy, for all $k = 1, ..., K$:

$$\frac{1}{n}\mathbb{E}(\|\mathbf{x}_k - \hat{\mathbf{x}}_k\|^2) \leq d. \tag{2.3}$$

The IFSC scheme discussed in this chapter tries to supply the encoding and decoding functions such that (2.3) holds, and can be summarized as follows. Using a nested lattice pair that all encoders and the decoder have access to, each encoder quantizes its observations to a fine lattice that works as a vector quantizer, and then reduces that quantized point modulo a coarse lattice performing a binning operation. The resulting point is then transmitted and the decoder uses the correlation between the original observations to guess in which bin the quantized signal originally was, estimating, if successful, the original point plus a quantization error induced by the quantization process at the encoders. Due to this dependency of the encoding/decoding process on nested lattice pairs, it is paramount to first introduce the necessary lattice theory for the formulation of the IFSC scheme.

2.2 Lattice Theory and Properties

As was previoulsy stated, lattice theory plays a key role in the formulation of the IFSC scheme. In this section, some basic lattice theory is explained as well as some properties that are of interest to this scheme.

From a mathematical point of view, a lattice Λ is a discrete sub-group of $\mathbb{R}^n$ that is closed under reflection and real addition as stated in [31]. It is discrete in the sense that the distance between any two lattice points is greater than some positive number. Closed under reflection because if λ is a lattice point then so is its reflection $-\lambda$, and under real addition because if two points λ_1 and λ_2 are lattice points so is their vector sum $\lambda_1 + \lambda_2$. These lattice properties are exemplified in figure 2.3. Moreover, a lattice is a countably infinite set because it must contain all integer multiples of any lattice point λ, as well as all integer linear combinations of any two lattice points λ_1 and λ_2. This is the reason why the zero point is always a lattice point, because for any lattice point λ one has the integer linear combination $\lambda + (-\lambda) = 0$.

It is possible to define a lattice in terms of a vector basis [31]: a n-dimensional lattice Λ is defined by a set of n linearly independent basis column vectors $\mathbf{g}_1, ..., \mathbf{g}_n \in \mathbb{R}^{n\times 1}$. The lattice Λ amounts to all

integer linear combinations of the basis vectors:

$$\Lambda(\mathbf{G}) = \{\lambda = \mathbf{G}\mathbf{i} : \mathbf{i} \in \mathbb{Z}^n\}, \tag{2.4}$$

where $\mathbf{i} = [i_1 \cdots i_n]^T$ is an n-dimensional integer column vector and $\mathbf{G} = [\mathbf{g}_1 \cdots \mathbf{g}_n]$ the $n \times n$ generator matrix.

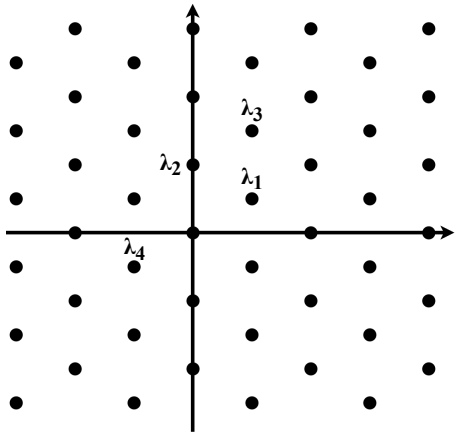


Figure 2.3: A 2-dimensional lattice. The lattice is closed under real addition (e.g., $\lambda_3 = \lambda_1 + \lambda_2$) and under reflection (e.g., $\lambda_4 = -\lambda_1$).

It is important to note that this generator matrix is not unique for a given lattice. In fact, a matrix $\mathbf{G}'$ generates the same lattice as $\mathbf{G}$, i.e., $\Lambda(\mathbf{G}) = \Lambda(\mathbf{G}')$ if

$$\mathbf{G}' = \mathbf{G}\mathbf{T}, \tag{2.5}$$

where $\mathbf{T}$ is an unimodular matrix, i.e., an integer valued matrix with a unit absolute determinant, $\det(\mathbf{T}) = \pm 1$. In fact, the more general relation between equivalent lattices also accomodate an orthogonal rotation performed by an orthogonal matrix $\mathbf{Q}$ such that

$$\mathbf{G}' = \mathbf{Q}\mathbf{G}\mathbf{T}, \tag{2.6}$$

that is, one says that a rotated version of a lattice in space is the same lattice. An example of different basis vectors is depicted in figure 2.4 where two different generator matrices generate the same lattice. The fact that the basis for a lattice is not unique gives rise to the question of what basis is the best basis for a given lattice. Although this is not precise, there are two common rules for a "good basis" [31]

1. the basis vectors $\mathbf{g}_1, ..., \mathbf{g}_n$ are as short as possible;

2. the basis vectors are nearly orthogonal.

These two rules are useful when tackling the problem of finding the closest lattice point to a given lattice point, and in lattice reduction, i.e., finding a "shorter" and more orthogonal basis of a given lattice. The LLL algorithm [26, 27] performs this basis reduction and will be useful in the sequel.

Another useful definition for the purposes of this thesis is the one for the successive minima (SM) of a lattice Λ provided in [32]. The kth successive minimum $\theta_k(\Lambda)$ of a lattice Λ is the smallest real number such that there are k linearly independent vectors in Λ of length at most $\theta_k(\Lambda)$. Clearly the K successive minima of a K- dimensional lattice obey

$$\theta_1(\Lambda) \leq \theta_2(\Lambda) \leq ... \leq \theta_K(\Lambda). \tag{2.7}$$

Geometrically one has that $\theta_k(\Lambda)$ is the smallest value r_k such that the closed K-dimensional ball centred at the origin $\mathbb{B}(\mathbf{0}, r_k) = \{\mathbf{x} \in \mathbb{R}^{K\times 1} : \|\mathbf{x}\| \leq r_k\}$ of radius r_k centered at the origin contains k linearly independent lattice points [33]. An example is provided in figure 2.5.

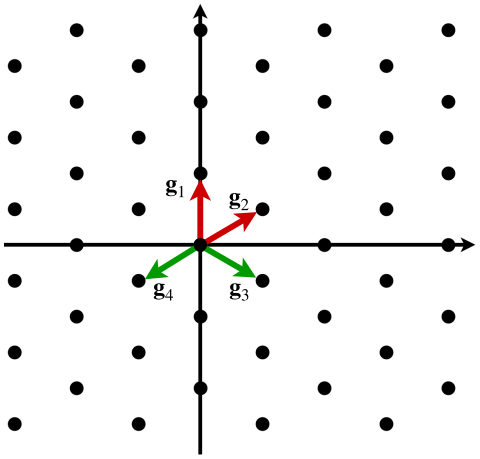


Figure 2.4: Vectors represented in red $\mathbf{g}_1 = [0\ 2]^T$ and $\mathbf{g}_2 = [\sqrt{3}\ 1]^T$ constitute a generator matrix $\mathbf{G}$. Vectors represented in green $\mathbf{g}_3 = [\sqrt{3}\ -1]^T$ and $\mathbf{g}_4 = [-\sqrt{3}\ -1]^T$ constitute a generator matrix $\mathbf{G}'$. $\mathbf{G}$ and $\mathbf{G}'$ generate the same 2-dimensional hexagonal lattice denoted as A_2 [31].

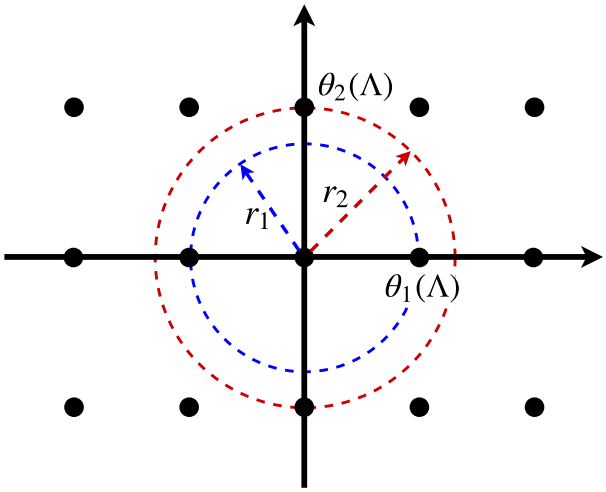


Figure 2.5: Example of the successive minima in a 2-dimensional lattice. $\theta_1(\Lambda)$ is the smallest value such that the circle defined by $\mathbb{B}(\mathbf{0}, r_1)$ contains one linearly independent lattice point. Similarly, $\theta_2(\Lambda)$ is the smallest value such that the circle defined by $\mathbb{B}(\mathbf{0}, r_2)$ contains two linearly independent lattice points as $\theta_1(\Lambda)$ and $\theta_2(\Lambda)$.

A relevant feature of lattices that is of great use to the IFSC scheme is that a lattice Λ can be used

to quantize continuous sources [31]. Considering a source $\mathbf{y} \in \mathbb{R}^{1\times n}$, an encoder that is interested in transmitting this source to a decoder can first quantize $\mathbf{y}$ onto the lattice Λ, $Q_\Lambda(\mathbf{y})$, and send a description of this point to the decoder. The nearest neighbour quantizer associated with the lattice Λ is defined by

$$Q_\Lambda(\mathbf{y}) = \arg\min_{\lambda\in\Lambda} \|\mathbf{y} - \lambda\|, \tag{2.8}$$

where $\|\cdot\|$ denotes the Euclidean distance between two vectors. The modulo-Λ operation on $\mathbf{y}$ returns the quantization error vector $\mathbf{e}$ with respect to the lattice Λ,

$$\mathbf{e} = [\mathbf{y}] \bmod \Lambda = \mathbf{y} - Q_\Lambda(\mathbf{y}). \tag{2.9}$$

The relationship expressed by (2.9) is represented in figure 2.6 where $\mathbb{R}^2$ was partitioned using a Voronoi partition, as defined in the following. Each partition cell P_λ of a lattice point λ is given by

$$P_\lambda = P_0 + \lambda = \{\mathbf{y} : (\mathbf{y} - \lambda) \in P_0\}, \tag{2.10}$$

where

$$P_0 = \{\mathbf{y} : \|\mathbf{y}\| \leq \|\mathbf{y} - \lambda\|, \forall\, \lambda \in \Lambda \setminus \{\mathbf{0}\}\} \tag{2.11}$$

is the partition cell of the zero point that, if expressed as in (2.11), can also be called the basic Voronoi region, i.e., the set of all points in $\mathbb{R}^n$ which are quantized to the zero point. This region is highlighted in figure 2.6 and for the remaining of this thesis it will be denoted by $\mathcal{V}$. Vol$(\mathcal{V})$ denotes the volume of the Voronoi region $\mathcal{V}$ of a lattice Λ, and $r_{eff}(\Lambda)$ the effective radius of Λ that corresponds to a n-dimensional ball whose volume equals Vol$(\mathcal{V})$.

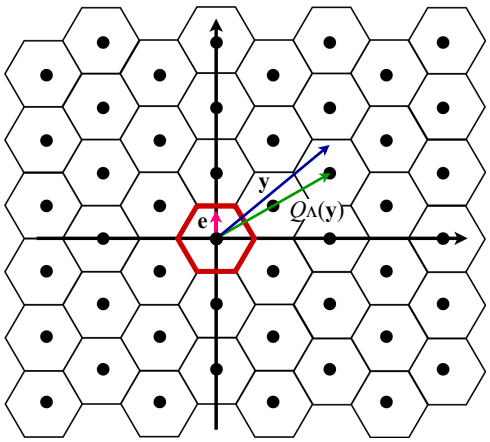


Figure 2.6: The difference between the vector $\mathbf{y}$ (in blue) and its nearest neighbour quantization associated with lattice Λ, $Q_\Lambda(\mathbf{y})$ (in green), is equal to the quantization error $\mathbf{e}$ (in pink). The basic Voronoi region $\mathcal{V}$ corresponds to the area contained by the edges highlighted in red.

The quantization error $\mathbf{e}$ of equation (2.9) is dependent on the original source $\mathbf{y}$ but can be made statistically independent with the introduction of some common randomness known to both the encoders and the decoder. This is performed with the use of a dithered quantization[2] scheme represented in figure

[2]For an introduction to the role of dithering in quantization, the reader is referred to the article [34].

2.7 where a random dither vector $\mathbf{d}$ that is uniformly distributed over $\mathcal{V}$ and statistically independent of $\mathbf{y}$ is used. The quantizer computes $Q_\Lambda(\mathbf{y}+\mathbf{d})$ and sends a description of the obtained lattice point to the decoder that creates an estimate given by

$$\begin{aligned}\hat{\mathbf{y}} &= Q_\Lambda(\mathbf{y}+\mathbf{d}) - \mathbf{d} \\ &= \mathbf{y} + Q_\Lambda(\mathbf{y}+\mathbf{d}) - (\mathbf{y}+\mathbf{d}) \\ &= \mathbf{y} - [\mathbf{y}+\mathbf{d}] \bmod \Lambda,\end{aligned} \tag{2.12}$$

where

$$\begin{aligned}\mathbf{u} &= Q_\Lambda(\mathbf{y}+\mathbf{d}) - (\mathbf{y}+\mathbf{d}) \\ &= -[\mathbf{y}+\mathbf{d}] \bmod \Lambda\end{aligned} \tag{2.13}$$

is the estimation error. It should be noted though, that in general, for any given lattice, the quantization operation is not computationally trivial. It is well-known that, for a given general lattice, the closest vector problem (CVP) belongs to the complexity class of the NP-hard problems.

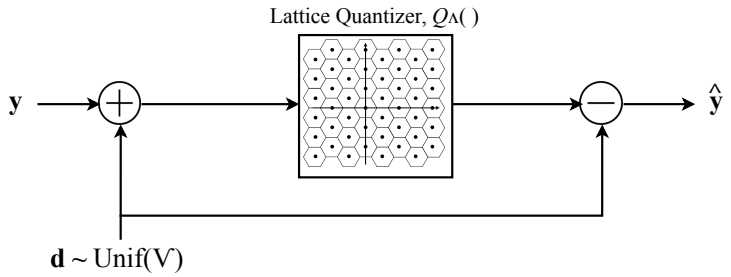


Figure 2.7: Dithered lattice quantization scheme.

The Crypto Lemma of [35] states that if $\mathbf{d}$ is uniformly distributed over $\mathcal{V}$, i.e., $\mathbf{d} \sim \mathsf{Unif}(\mathcal{V})$, then

$$[\mathbf{y}+\mathbf{d}] \bmod \Lambda \sim \mathsf{Unif}(\mathcal{V}), \forall\, \mathbf{y}. \tag{2.14}$$

From (2.13) one can also conclude that

$$\mathbf{u} \sim \mathsf{Unif}(\mathcal{V}), \forall\, \mathbf{y}. \tag{2.15}$$

This ensures that the estimation error $\mathbf{u}$ is statistically independent of $\mathbf{y}$ and uniformly distributed over $\mathcal{V}$ which will also be useful for the formulation of the simpler IFSC scheme in chapter 5. The mean square error (MSE) per dimension attained by this dithered lattice quantization scheme is given by

$$\begin{aligned}\frac{1}{n}\mathbb{E}(\|\mathbf{y}-\hat{\mathbf{y}}\|^2) &= \frac{1}{n}\mathbb{E}(\|\mathbf{u}\|^2) \\ &= \sigma^2(\Lambda),\end{aligned} \tag{2.16}$$

where $\sigma^2(\Lambda)$ is the second moment of Λ defined as

$$\sigma^2(\Lambda) = \frac{1}{n}\frac{1}{\text{Vol}(\mathcal{V})}\int_{\mathcal{V}} \|\mathbf{u}\|^2 \, d\mathbf{u}. \tag{2.17}$$

The main issue regarding the described dithered lattice quantization scheme as a stand-alone quantization scheme is that, since the encoder needs all the points in Λ available to quantize a observation $\mathbf{y}$, and given that Λ by construction has an infinite number of points, an infinite rate would be required. To bypass this problem, a nested lattice codebook is considered [24].

A pair of n-dimensional lattices Λ_1 and Λ_2 is said to be nested if $\Lambda_2 \subset \Lambda_1$, i.e., Λ_2 is a sub-lattice of Λ_1. Λ_2 is referred to as the *coarse lattice* denoted by Λ_c, and Λ_1 as the *fine lattice* denoted by Λ_f. An example of two nested lattices is represented in figure 2.8. The fundamental partition P_0 of a coarse lattice Λ_c that is part of a general nested lattice pair can shape a codebook consisting of the fine lattice points that are contained in this fundamental partition. This is the basic idea behind a nested lattice codebook [16]. In a precise definition, for a pair of nested lattices, a lattice-shaped codebook is the intersection of Λ_f with a fundamental partition of Λ_c,

$$\mathcal{C} = \Lambda_f \cap P_0(\Lambda_c). \tag{2.18}$$

If the fundamental partition $P_0(\Lambda_c)$ corresponds to the basic Voronoi region of Λ_c, $\mathcal{V}(\Lambda_c)$, then the lattice-shaped codebook of equation (2.18) is called a Voronoi codebook. An example of this particular type of codebook is depicted in figure 2.8, where the fine lattice points contained by the basic Voronoi region of the coarse lattice correspond to the codewords belonging to the codebook. It is this type of codebook that the IFSC scheme implements.

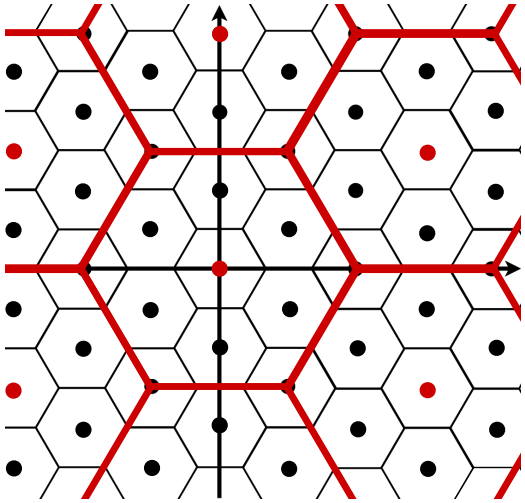


Figure 2.8: Two nested 2-dimensional hexagonal lattices. The points that belong to the coarse lattice Λ_c are represented in red as well as their corresponding Voronoi partitions. The points of the fine lattice Λ_f are in black as well as their corresponding Voronoi partitions. It is important to note that all the points of Λ_c are also points of Λ_f.

The rate R of such an n-dimensional code C with M equally likely codewords is given by

$$R = \frac{1}{n}\log_2(M). \tag{2.19}$$

The number of codewords M can be expressed by

$$M = \frac{\mathsf{Vol}(\Lambda_c)}{\mathsf{Vol}(\Lambda_f)}, \tag{2.20}$$

where $\mathsf{Vol}(\Lambda_c)$ and $\mathsf{Vol}(\Lambda_f)$ are, respectively, the volumes of an individual partition of the coarse and fine lattice. Plugging (2.20) into (2.19) yields

$$R = \frac{1}{n}\log_2\left(\frac{\mathsf{Vol}(\Lambda_c)}{\mathsf{Vol}(\Lambda_f)}\right). \tag{2.21}$$

Furthermore, if one considers that the volume of an n-dimensional sphere is

$$\mathsf{Vol}_n = c_n \cdot \pi^{\frac{n}{2}} \cdot r^n, \tag{2.22}$$

where c_n is some coefficient for the dimension n, and r is the radius of the n-dimensional sphere, one can state that

$$\mathsf{Vol}(\Lambda) = c_n \cdot \pi^{\frac{n}{2}} \cdot r_{eff}^n(\Lambda). \tag{2.23}$$

Inserting expression (2.23) in (2.21) one obtains a useful expression for the rate of a nested lattice codebook

$$\begin{aligned} R &= \frac{1}{n}\log_2\left(\frac{c_n \cdot \pi^{\frac{n}{2}} \cdot r_{eff}^n(\Lambda_c)}{c_n \cdot \pi^{\frac{n}{2}} \cdot r_{eff}^n(\Lambda_f)}\right) \\ &= \log_2\left(\frac{r_{eff}(\Lambda_c)}{r_{eff}(\Lambda_f)}\right) \\ &= \frac{1}{2}\log_2\left(\frac{r_{eff}^2(\Lambda_c)}{r_{eff}^2(\Lambda_f)}\right). \end{aligned} \tag{2.24}$$

Before closing this section and moving on to the IFSC scheme, it is important to mention that the nested lattice pair used in this scheme needs to satisfy some lattice "goodness" properties as stated by [24]. The fine lattice Λ_f has to be *good for MSE quantization*, and the coarse lattice Λ_c has to be *good for channel coding*. These two definitions (available in [31] and [16]) are important to the IFSC scheme and are both presented in more detail in appendix A. Although this is not in the main scope of this thesis, an ensemble of nested lattice pairs that satisfy these lattice goodness properties can be consulted in [36].

2.3 Integer-Forcing Source Coding

The IFSC scheme is presented in this section in a manner that closely follows [24]. First, an overview of the scheme is provided where the lattice properties presented in the last section are applied in the IFSC

context. Then, an analysis of the performance with respect to the rate-distortion vector attainable with this scheme is made. To conclude this section a replication of the results obtained in [24] is presented.

2.3.1 Overview of the Integer-Forcing Source Coding scheme

As previoulsy mentioned, the IFSC scheme proposed in [24] follows the ideia behind IF linear receivers for MIMO communications [21], where the receiver decodes integer linear combinations of the transmitted codewords in order to estimate the original signals. This is only possible if all the encoders and the decoder use the same linear code. Similarly, a prerequisite for the IFSC scheme is that all the encoders and the decoder have a shared knowledge of the same nested lattice codebook $\mathcal{C} = \Lambda_f \cap \mathcal{V}(\Lambda_c)$. The rate of such codebook is given by expression (2.24), while it is assumed that the fine lattice Λ_f is good for MSE quantization and the coarse lattice Λ_c is good for channel coding (cf. appendix A). Λ_f has a second moment $\sigma^2(\Lambda_f) = d$, where d can be seen as the variance of the quantization distortion irreversibly added in the quantization process by the encoders.

All encoders in this scheme employ the same encoding operation. The kth encoder uses a dither vector $\mathbf{d}_k$ statistically independent of the sources $\mathbf{x}_k$ and uniformly distributed over the basic Voronoi region of Λ_f, $\mathcal{V}(\Lambda_f)$, and performs dithered quantization of $\mathbf{x}_k$ onto Λ_f. Next, it reduces the obtained point modulo-Λ_c to obtain

$$\left[Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k)\right] \bmod \Lambda_c,$$

which belongs to the codebook $\mathcal{C}$. As mentioned before, this modulo reduction amounts to a binning operation, and, consequently, the encoder only transmits the least significant bits (LSBs) of the dithered quantization of the original source $\mathbf{x}_k$. These nR bits that describe the modulo reduced point are then sent to the decoder in the other terminal. The just described encoding process is exemplified in figure 2.9 with the help of the 2-dimensional nested lattice pair of figure 2.8.

At the other terminal, the decoder, having full knowledge about the dither vector $\mathbf{d}_k$ added at the encoder's side, subtracts it back and reduces the result modulo-Λ_c resulting in

$$\begin{aligned}
\tilde{\mathbf{x}}_k &= \left[\left[Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k)\right] \bmod \Lambda_c - \mathbf{d}_k\right] \bmod \Lambda_c \\
&= \left[Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k) - \mathbf{d}_k\right] \bmod \Lambda_c \\
&= \left[\mathbf{x}_k + Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k) - (\mathbf{x}_k + \mathbf{d}_k)\right] \bmod \Lambda_c \\
&= \left[\mathbf{x}_k + \mathbf{u}_k\right] \bmod \Lambda_c,
\end{aligned} \tag{2.25}$$

where the second equality follows from the distributive law (cf. appendix B) and $\mathbf{u}_k$ is the estimation error given by

$$\mathbf{u}_k = Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k) - (\mathbf{x}_k + \mathbf{d}_k). \tag{2.26}$$

This estimation error is, as a consequence of the Crypto Lemma presented in section 2.2, uniformly distributed over the Voronoi region of the fine lattice Λ_f and statistically independent of $\mathbf{x}_k$ for all $k = 1, ..., K$. This part of the decoder's operation is represented in figure 2.10, where some of the intermediate vectors are the ones depicted in figure 2.9.

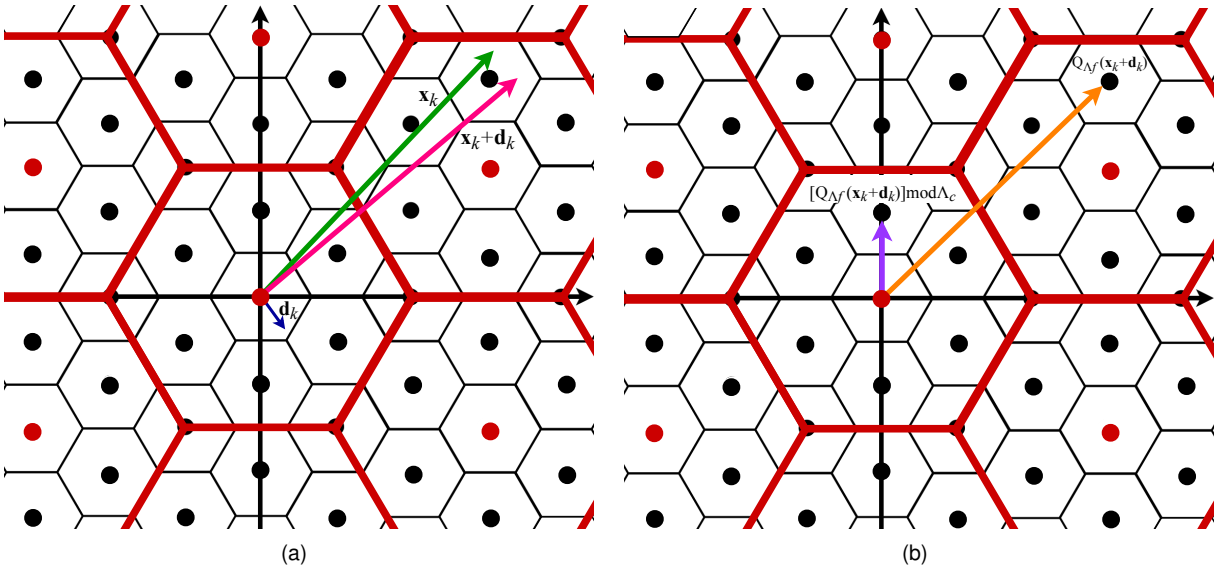


Figure 2.9: Dithered lattice quantization process and modulo reduction in the encoding operation. (a) The dither vector $\mathbf{d}_k$ (in blue) is added to the source vector $\mathbf{x}_k$ (in green), resulting in the vector $\mathbf{x}_k + \mathbf{d}_k$ (in pink). (b) The resulting vector is then quantized onto the fine lattice Λ_f to obtain $Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k)$ (in orange), which in turn is reduced modulo the coarse lattice Λ_c to get $\left[Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k)\right] \mod \Lambda_c$ (in purple).

Choosing the coarse lattice Λ_c with effective radius $r_{eff}(\Lambda_c)$ large enough to contain the sum $\mathbf{x}_k + \mathbf{u}_k$, the final modulo-$\Lambda_c$ reduction in (2.25) has no effect and so, recalling expression (2.17) for the average MSE per dimension attained by the dithered lattice quantization, one obtains

$$\begin{aligned} \frac{1}{n}\mathbb{E}(\|\mathbf{x}_k - \hat{\mathbf{x}}_k\|^2) &= \frac{1}{n}\mathbb{E}(\|\mathbf{u}_k\|^2) \\ &= \sigma^2(\Lambda) \\ &= d, \end{aligned} \tag{2.27}$$

as desired.

The problem with this first approach is that since the rate R grows with $r_{eff}(\Lambda_c)$ according to (2.24), it is desired to have it as small as possible. To address this problem, the main feature of IFSC is applied as follows. If the elements of $\mathbf{x} = [x_1 \cdots x_K]^T \in \mathbb{R}^{K\times 1}$ present a correlation expressed by a covariance matrix obtained through (2.1), then linear combinations of the vectors $\mathbf{x}_k + \mathbf{u}_k$, for $k = 1, ..., K$, with integer-valued coefficients may have a smaller variance than the original $\mathbf{x}_k + \mathbf{u}_k$. These integer-valued coefficients take a form of an integer-valued matrix $\mathbf{A} \in \mathbb{Z}^{K\times K}$ that depends on the covariance matrix $\mathbf{K_{xx}}$, as one will see in the sequel. If chosen appropriately, the integer-valued matrix $\mathbf{A}$ combined with $\mathbf{X} + \mathbf{U}$, where $\mathbf{X} = [\mathbf{x}_1^T \cdots \mathbf{x}_K^T]^T$ and $\mathbf{U} = [\mathbf{u}_1^T \cdots \mathbf{u}_K^T]^T$ are both $K \times n$ matrices, has the effect of "enclosing" $\mathbf{X} + \mathbf{U}$ in the basic Voronoi region of Λ_c. This effect is exemplified with the plots presented in figures 2.11 and 2.12 where the partitions of Λ_c take the shape of a square area. This choice of a square area as the partition of Λ_c only serves the purpose of illustrating the effect of $\mathbf{A}$. By using this property, $r_{eff}(\Lambda_c)$ only needs to be greater than the largest variance among the K integer linear combinations. If the elements of $\mathbf{x} = [x_1 \cdots x_K]^T \in \mathbb{R}^{K\times 1}$ are sufficiently correlated and the integer-valued matrix $\mathbf{A}$ is chosen appropriately, this "enclosing" effect can be explored to reduce $r_{eff}(\Lambda_c)$, and as a consequence

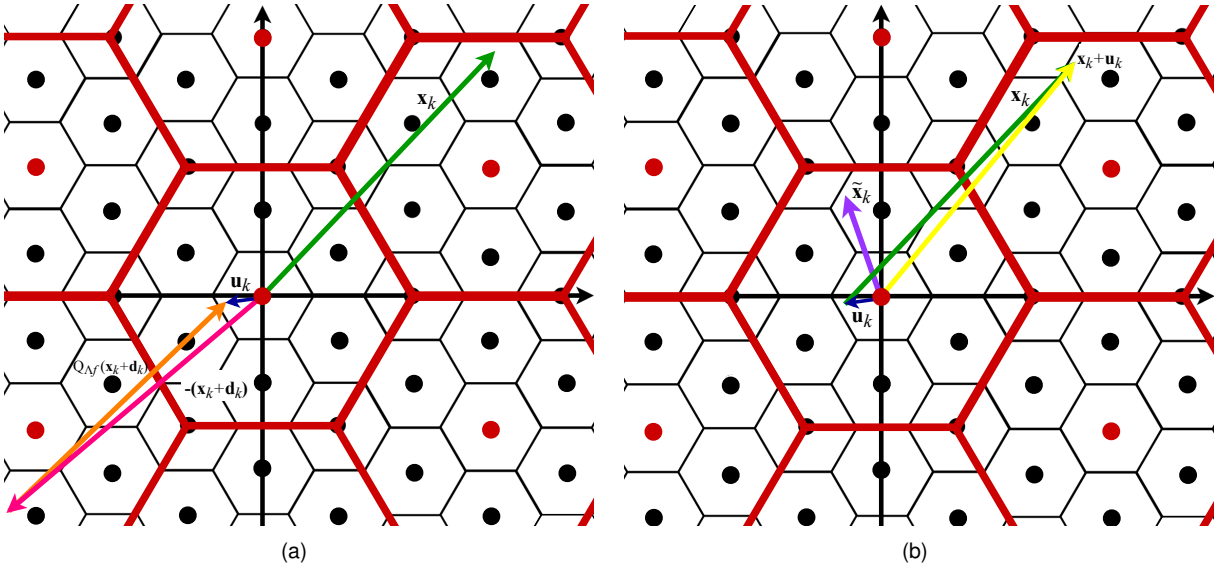


Figure 2.10: Estimation error and modulo reduction in the decoding operation. (a) Random vector $\mathbf{u}_k$ (in blue) is equivalent to the vectorial sum of $Q_{\Lambda_f}(\mathbf{x}_k + \mathbf{d}_k)$ (in orange) with $-(\mathbf{x}_k + \mathbf{d}_k)$ (in pink) and is, as expected, inside $\mathcal{V}(\Lambda_f)$. (b) The sum of this vector $\mathbf{u}_k$ and the source vector $\mathbf{x}_k$ (in green) is $\mathbf{x}_k + \mathbf{u}_k$ (in yellow) and its modulo-Λ_c reduction is $\tilde{\mathbf{x}}_k$ (in purple).

of doing that the required coding rate may be significantly reduced.

Considering that $\tilde{\mathbf{X}} = [\tilde{\mathbf{x}}_1^T \cdots \tilde{\mathbf{x}}_K^T]^T$ is also a $K \times n$ matrix, the decoder has access to

$$\tilde{\mathbf{X}} = [\mathbf{X} + \mathbf{U}] \bmod \Lambda_c \tag{2.28}$$

where the modulo-Λ_c reduction is equivalent to reducing each row of the matrix $\mathbf{X} + \mathbf{U}$.

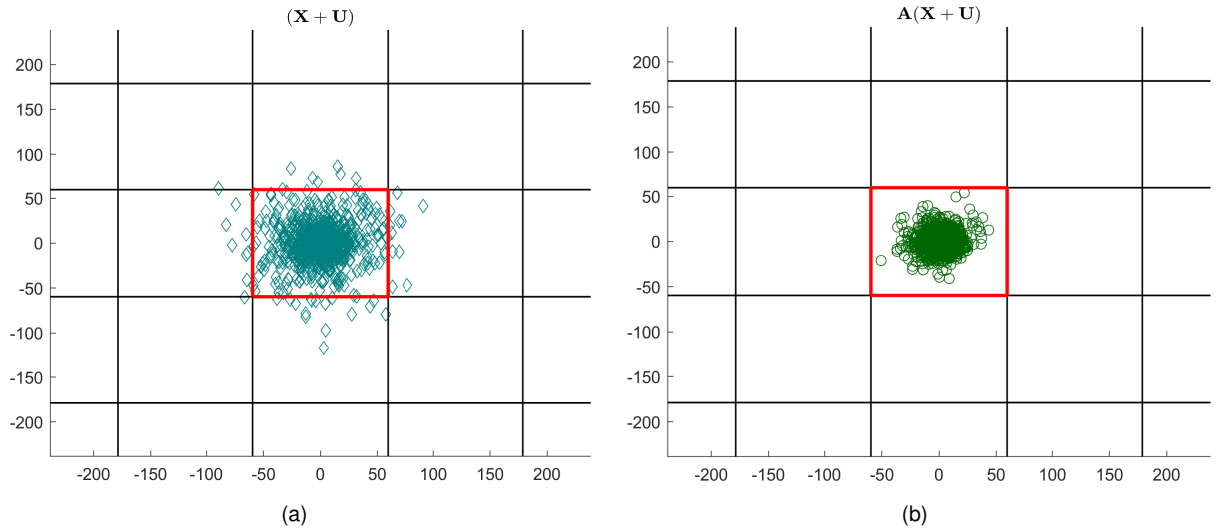


Figure 2.11: Successful example of the "enclosing" effect of the integer-valued matrix $\mathbf{A}$. (a) The 2-dimensional samples of $\mathbf{X}$ are correlated through a covariance matrix $\mathbf{K_{xx}}$, and the sum $(\mathbf{X} + \mathbf{U})$ is plotted. (b) The integer linear combinations between the elements of $(\mathbf{X} + \mathbf{U})$ with the aid of an appropriate integer-valued matrix $\mathbf{A}$ are enclosed in the basic Voronoi region of the coarse lattice highlighted in red.

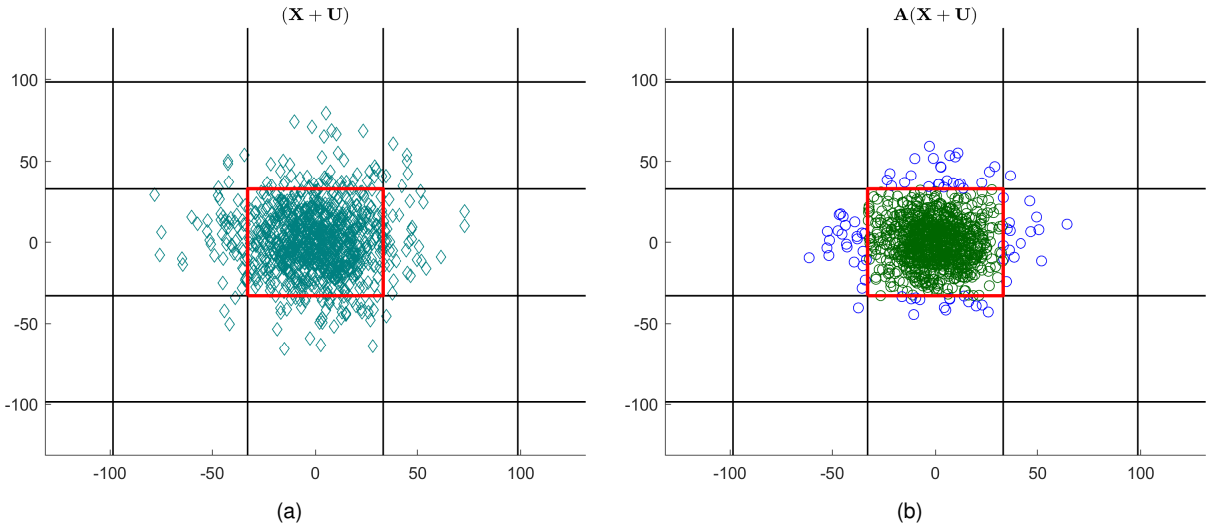


Figure 2.12: Unsuccessful example of the "enclosing" effect of the integer-valued matrix $\mathbf{A}$. (a) The 2-dimensional samples of $\mathbf{X}$ are correlated through a covariance matrix $\mathbf{K_{xx}}$, and the sum $(\mathbf{X}+\mathbf{U})$ is plotted. (b) The integer linear combinations between the elements of $(\mathbf{X}+\mathbf{U})$ with the aid of an appropriate integer-valued matrix $\mathbf{A}$ are closer to the basic Voronoi region of the coarse lattice highlighted in red but not confined by it since there are linear combinations that fall outside of this region (in blue).

With the precalculated full-rank integer-valued matrix $\mathbf{A}$, the decoder computes

$$\begin{aligned}\widehat{\mathbf{AX}} &\triangleq [\mathbf{A}\tilde{\mathbf{X}}] \bmod \Lambda_c \\ &= \big[\mathbf{A}\big([\mathbf{X}+\mathbf{U}] \bmod \Lambda_c\big)\big] \bmod \Lambda_c \\ &= \big[\mathbf{A}(\mathbf{X}+\mathbf{U})\big] \bmod \Lambda_c\end{aligned} \tag{2.29}$$

where the third equality follows from the "general" distributive law for matrices (cf. appendix B). This modulo-lattice property is of crucial importance to IFSC and in this context is summarized by the block diagrams of figure 2.13.

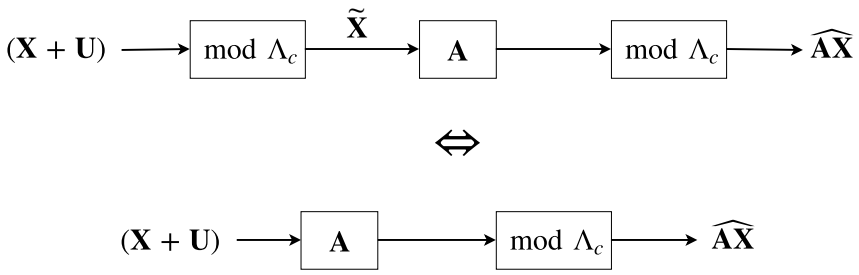


Figure 2.13: Equivalence allowed by the modulo-lattice properties.

Taking into account that $\mathbf{a}_k^T$ is the kth row of the matrix $\mathbf{A}$, $\mathbf{a}_k^T\mathbf{X}$ is a Gaussian vector. Each vector $\mathbf{u}_k$ for $k = 1, ..., K$ is uniformly distributed over $\mathcal{V}(\Lambda_f)$ of a lattice Λ_f that is good for MSE quantization. Therefore, according to the lemma available in appendix A, $\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})$ is semi norm-ergodic [24]. Using the definition for a lattice's goodness for channel coding (cf. appendix A), if the variance of a semi

norm-ergodic vector such as $\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})$ follows

$$\frac{\mathbb{E}(\left\|\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})\right\|^2)}{n} < \frac{r_{eff}^2(\Lambda_c)}{n}, \tag{2.30}$$

then

$$\lim_{n\to\infty} P\big(\mathbf{a}_k^T(\mathbf{X}+\mathbf{U}) \notin \mathcal{V}(\Lambda_c)\big) = 0, \tag{2.31}$$

which is equivalent to

$$\big[\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})\big] \bmod \Lambda_c = \mathbf{a}_k^T(\mathbf{X}+\mathbf{U}) \tag{2.32}$$

with high probability. Generalizing inequality (2.30) for all $k = 1, ..., K$, if

$$\max_{k=1,...,K} \frac{\mathbb{E}(\left\|\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})\right\|^2)}{n} < \frac{r_{eff}^2(\Lambda_c)}{n}, \tag{2.33}$$

then

$$\big[\mathbf{A}(\mathbf{X}+\mathbf{U})\big] \bmod \Lambda_c = \mathbf{A}(\mathbf{X}+\mathbf{U}) \tag{2.34}$$

with high probability and equation (2.29) turns into

$$\widehat{\mathbf{AX}} = \mathbf{A}(\mathbf{X}+\mathbf{U}). \tag{2.35}$$

The variance of the integer linear combinations between $\mathbf{X}+\mathbf{U}$ can be expressed by

$$\frac{\mathbb{E}(\left\|\mathbf{a}_k^T(\mathbf{X}+\mathbf{U})\right\|^2)}{n} = \mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k, \tag{2.36}$$

and so it is sufficient to set $r_{eff}^2(\Lambda_c)$ as the maximum of $\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k$ for all $k = 1, ..., K$ to achieve (2.35). By the definition for the lattice's goodness for MSE quantization (cf. appendix A), and recalling that $\sigma^2(\Lambda_f) = d$ one has

$$\frac{r_{eff}^2(\Lambda_f)}{n} \to d$$

when n approaches infinity. With all this in mind the attainable rate R for this scheme becomes

$$\begin{aligned} R &= \frac{1}{2}\log_2\left(\frac{r_{eff}^2(\Lambda_c)}{r_{eff}^2(\Lambda_f)}\right) \\ &= \frac{1}{2}\log_2\left(\frac{\frac{r_{eff}^2(\Lambda_c)}{n}}{\frac{r_{eff}^2(\Lambda_f)}{n}}\right) \\ &= \frac{1}{2}\log_2\left(\frac{\max_{k=1,...,K}\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k}{d}\right) \\ &= \frac{1}{2}\log_2\left(\max_{k=1,...,K}\mathbf{a}_k^T(\mathbf{I}+\frac{\mathbf{K_{xx}}}{d})\mathbf{a}_k\right). \end{aligned} \tag{2.37}$$

Finally, the decoder computes the estimates of $\mathbf{X}$ by applying the inverse matrix of $\mathbf{A}$ to (2.35)

obtaining

$$\begin{aligned}\widehat{\mathbf{X}} &= \mathbf{A}^{-1}\widehat{\mathbf{A}\mathbf{X}} \\ &= \mathbf{X} + \mathbf{U}.\end{aligned} \tag{2.38}$$

It is this decoder operation that sets the requirement for $\mathbf{A}$ to be an invertible matrix and therefore it is a full-rank matrix, i.e., it has K linearly independent columns.

The final MSE attained by this scheme is then

$$\frac{1}{n}\mathbb{E}(\|\hat{\mathbf{x}}_k - \mathbf{x}_k\|^2) = d, \tag{2.39}$$

which is obtained when n approaches infinity.

The above described decoding process can be seen from a general perspective as the decoder using the correlation between the sources through $\mathbf{A}$ to return a best guess of the bin in which the quantized source originally was, and by that process estimating the most significant bits (MSBs) of that quantized source. Since this is a lossy distributed source coding scheme, even in the event of success, i.e., if the decoder can guess correctly the original partition of Λ_c (the correct bin), because the integer linear combinations between $\mathbf{x}_k + \mathbf{u}_k$ are inside $\mathcal{V}(\Lambda_c)$ (as represented in figure 2.11), and the modulo-Λ_c in (2.29) is redundant, there is no way of avoiding the quantization error introduced at the encoders in the dithered lattice quantization. It is also important to note that if the integer linear combinations between $\mathbf{x}_k + \mathbf{u}_k$ are outside $\mathcal{V}(\Lambda_c)$ (as represented in figure 2.12) the decoder fails to recover those MSBs.

The block diagram of the IFSC scheme described in this section is depicted in figure 2.14.

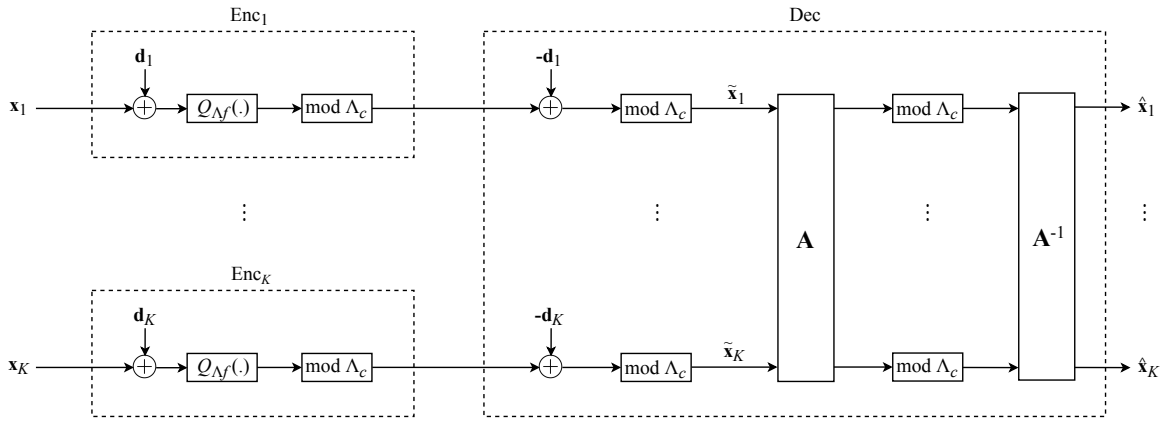


Figure 2.14: Integer-forcing source coding scheme.

2.3.2 Performance of the Integer-Forcing Source Coding scheme

The performance of the IFSC scheme is analysed with respect to the rate-distortion vector (R, d) it achieves for the symmetric rate setup. For any distortion $d > 0$ and any full-rank integer-valued matrix

$\mathbf{A}$ there exists a nested lattice pair such that this scheme can achieve any rate R that satisfies

$$R > R_{IFSC}(\mathbf{A}, d) \triangleq \frac{1}{2}\log_2\left(\max_{k=1,\ldots,K} \mathbf{a}_k^T(\mathbf{I} + \frac{\mathbf{K_{xx}}}{d})\mathbf{a}_k\right). \tag{2.40}$$

By choosing the full-rank integer-valued matrix $\mathbf{A}$ appropriately, the quadratic form inside the logarithm in (2.40) is minimized due to the "enclosing" effect described in the previous section, and $R_{IFSC}(\mathbf{A}, d)$ is also minimized, which amounts to the required rate to achieve a maximum distortion d when using the chosen $\mathbf{A}$. Therefore, one wants to choose an $\mathbf{A}$ such that (2.40) translates to

$$R > R_{IFSC}(d) \triangleq \frac{1}{2}\log_2\left[\min_{\substack{\mathbf{A}\in\mathbb{Z}^{K\times K}\\ \det(\mathbf{A})\neq 0}}\left(\max_{k=1,\ldots,K} \mathbf{a}_k^T(\mathbf{I} + \frac{\mathbf{K_{xx}}}{d})\mathbf{a}_k\right)\right]. \tag{2.41}$$

The optimal matrix $\mathbf{A}$ that solves the optimization problem inside the logarithm operation will be henceforth denoted by $\mathbf{A}^*$. Finding this optimal $\mathbf{A}^*$ is a problem that can itself be translated to the language of lattice problems, as it will be shown in the following.

Let a vector $\mathbf{y} \in \mathbb{Z}^{K\times 1}$ correspond to a lattice Λ point. Then, recalling the definition of a lattice with a fundamental basis given by (2.4), one has that $\mathbf{y}$ can be expressed as

$$\mathbf{y} = \mathbf{P}\mathbf{v}, \tag{2.42}$$

where $\mathbf{P}$ is a $K \times K$ lattice generator matrix and $\mathbf{v} = [v_1 \cdots v_K]^T \in \mathbb{Z}^{K\times 1}$ is a K-dimensional integer valued column vector the spans the lattice point $\mathbf{y} \in \Lambda(\mathbf{P})$. If one takes the inner product of $\mathbf{y}$ with itself one has that

$$\begin{aligned}\langle \mathbf{y}, \mathbf{y}\rangle &= \|\mathbf{y}\|^2 \\ &= \mathbf{y}^T\mathbf{y} \\ &= (\mathbf{P}\mathbf{v})^T\mathbf{P}\mathbf{v} \\ &= \mathbf{v}^T\mathbf{P}^T\mathbf{P}\mathbf{v},\end{aligned} \tag{2.43}$$

where $\mathbf{P}^T\mathbf{P}$ is a Gram matrix that shall be denoted by $\mathbf{G}$. This Gram matrix is symmetric and positive definite with $\det(\mathbf{G}) > 0$ and so it admits a Cholesky decomposition given by

$$\mathbf{G} = \mathbf{R}^T\mathbf{R}, \tag{2.44}$$

where $\mathbf{R}^T$ is a lower triangular matrix with strictly positive diagonal entries and $\mathbf{R}$ an upper triangular matrix with strictly positive diagonal entries. If one takes $\mathbf{v}$ to be equal to $\mathbf{a}_k$, the transpose of the kth row of $\mathbf{A}$, one obtains

$$\begin{aligned}\|\mathbf{y}\|^2 &= \mathbf{a}_k^T\mathbf{P}^T\mathbf{P}\mathbf{a}_k \\ &= \mathbf{a}_k^T\mathbf{G}\mathbf{a}_k.\end{aligned} \tag{2.45}$$

Setting

$$\mathbf{a}_k^T \mathbf{G} \mathbf{a}_k = \mathbf{a}_k^T (\mathbf{I} + \frac{\mathbf{K_{xx}}}{d}) \mathbf{a}_k, \tag{2.46}$$

it is possible to state that $\mathbf{I} + \frac{\mathbf{K_{xx}}}{d}$ admits a Cholesky decomposition as in (2.44). Taking this into account along with expressions (2.42) and (2.45) it is possible to update expression (2.41) to

$$\begin{aligned} R_{IFSC}(d) &\triangleq \frac{1}{2} \log_2 \left[\min_{\substack{\mathbf{A} \in \mathbb{Z}^{K \times K} \\ \det(\mathbf{A}) \neq 0}} \left(\max_{k=1,\ldots,K} \|\mathbf{y}_k\|^2 \right) \right] \\ &= \frac{1}{2} \log_2 \left[\min_{\substack{\mathbf{A} \in \mathbb{Z}^{K \times K} \\ \det(\mathbf{A}) \neq 0}} \left(\max_{k=1,\ldots,K} \|\mathbf{R}\mathbf{a}_k\|^2 \right) \right]. \end{aligned} \tag{2.47}$$

The problem of finding the optimal matrix $\mathbf{A}^*$ comes down to finding the K linearly independent vectors $\mathbf{a}_k^*$ that span the shortest lattice points $\mathbf{y}_k$ of a lattice Λ generated by a matrix $\mathbf{R}$. This problem is refered to as the shortest independent vectors problem (SIVP) [21] and it is also known to be a NP-hard problem. An approximate solution to this problem can be found using the LLL algorithm [26, 27] in polynomial running time. The LLL algorithm receives as an input a lattice generator matrix like $\mathbf{R}$ and returns a reduced generator matrix $\mathbf{R}_{red}$. This reduced generator matrix is constituted by basis vectors that follow the two rules for a good basis mentioned in section 2.2. $\mathbf{R}_{red}$ generates the same lattice as $\mathbf{R}$, i.e., $\Lambda(\mathbf{R}_{red}) = \Lambda(\mathbf{R})$, and the relationship between these two matrices is given by

$$\mathbf{R}_{red} = \mathbf{R}\mathbf{T}, \tag{2.48}$$

where $\mathbf{T} \in \mathbb{Z}^{K \times K}$ is an integer-valued unimodular matrix and represents an approximate solution of the optimal matrix $\mathbf{A}^*$, since the K columns of $\mathbf{R}_{red}$ can be seen as the K linearly independent shortest lattice points of $\mathbf{R}$.

The use of the LLL algorithm to solve the SIVP provides a good approximated solution but as K increases, i.e., the number of encoders in the distributed source coding setup increases, the gap between this solution and the exact one becomes larger. This will be analysed in the next chapter.

2.3.3 Testbed and Benchmark

In order to obtain the rate-distortion curve given by expression (2.41), which indicates the required rate by the IFSC scheme to attain a maximum distortion d, an example is required to provide a correlation model for the encoder's observations. With the objective of replicating the results obtained in [24], the same example was used, corresponding to compressing observations of correlated relays (encoders) in a Gaussian network depicted in figure 2.15. This Gaussian network consists of M non-cooperating transmitters each of which with a message w_m. The CP is interested in decoding all M messages even though it does not have direct access to those messages. Instead, there are K relays, each holding an observation of a noisy linear combination of the transmitted signals. These relays can be seen as the encoders and the CP as the decoder in the IFSC scheme.

The signal transmitted by the mth transmitter during n channel uses is $\mathbf{s}_m \in \mathbb{R}^{1 \times n}$ for $m = 1, ..., M$,

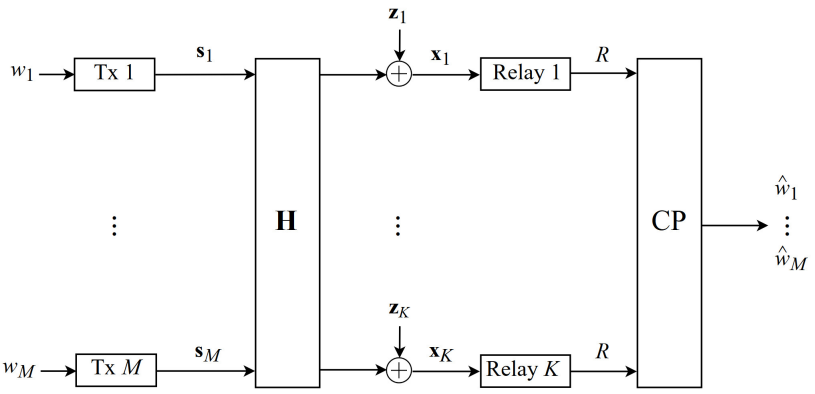


Figure 2.15: Gaussian network scheme with M transmitters and K relays.

and it is assumed that these signals statistically behave as white Gaussian noise and are subject to a power constraint given by

$$\mathbb{E}(\|\mathbf{s}_m\|^2) \leq n\text{SNR} \tag{2.49}$$

for a signal-to-noise ratio (SNR) that satisfies SNR > 0. Let $\mathbf{x}_k \in \mathbb{R}^{1\times n}$ be the signal received by the kth relay during n channel uses. Considering the matrices $\mathbf{S} = [\mathbf{s}_1^T \cdots \mathbf{s}_K^T]^T$ and $\mathbf{X} = [\mathbf{x}_1^T \cdots \mathbf{x}_K^T]^T$, the signals are related by

$$\mathbf{X} = \mathbf{HS} + \mathbf{Z}, \tag{2.50}$$

where the entries of $\mathbf{Z} \in \mathbb{R}^{K\times n}$ are i.i.d. with a Gaussian distribution $\mathcal{N}(0,1)$ and $\mathbf{H} \in \mathbb{R}^{K\times M}$ is the channel matrix between the M transmitters and the K relays. It is assumed that the entries of $\mathbf{H}$ are also i.i.d. with a Gaussian distribution $\mathcal{N}(0,1)$. The problem with such a Gaussian network scheme is that of compressing in a distributed way a K-dimensional Gaussian source $\mathbf{x}$ with zero mean and a covariance matrix given by

$$\mathbf{K_{xx}} = \text{SNR}\,\mathbf{HH}^T + \mathbf{I}. \tag{2.51}$$

To compare the performance of the IFSC scheme, a benchmark is defined in [24] as the rate-distortion vector attained from the best known achievable scheme for the problem of distributed lossy compression of jointly Gaussian random variables under a quadratic distortion measure, which is set by the Berger-Tung (BT) scheme [12, 37, 38]. As was exposed in the previous sections, the IFSC scheme relies on the use of integer linear combinations between the source plus an estimation error to return an estimate of the original source obtained with (2.38). This integer decoupling made at the decoder's side, if unsuccessful due for example to a poor choice of matrix $\mathbf{A}$, may lead to a total non-recovery of the original source. The Berger-Tung scheme does not rely on this integer decoupling and so it does not suffer from the errors it may lead to, attaining a better performance. However, to do so the Berger-Tung scheme presents an increased overall complexity that is required both at the encoders and at the decoder, in contrast to the IFSC scheme, where the processing is mostly done at the decoder. The Berger-Tung benchmark for symmetric rate-distortion normalized by K used for comparison is given in

[24] by

$$R_{BT}(d) \triangleq \frac{1}{2K}\log_2 \det\Big(\mathbf{I}+\frac{1}{d}\mathbf{K_{xx}}\Big). \tag{2.52}$$

To further assess the performance of the IFSC, it will also be considered in this comparison the rate-distortion vector obtained with a scheme that compresses each source without exploiting the correlation between the sources. This is equivalent to performing the IFSC process with an identity matrix, $\mathbf{A}^* = \mathbf{I}$, and, as in [24], this scheme is denoted has the *naive scheme*. The rate for this scheme is given by

$$R_{Naive}(d) \triangleq \max_{k=1,\ldots,K} \frac{1}{2}\log_2\left(1+\frac{\mathbf{K_{xx}}(k,k)}{d}\right), \tag{2.53}$$

where $\mathbf{K_{xx}}(k,k)$ is the kth diagonal entry of the matrix $\mathbf{K_{xx}}$.

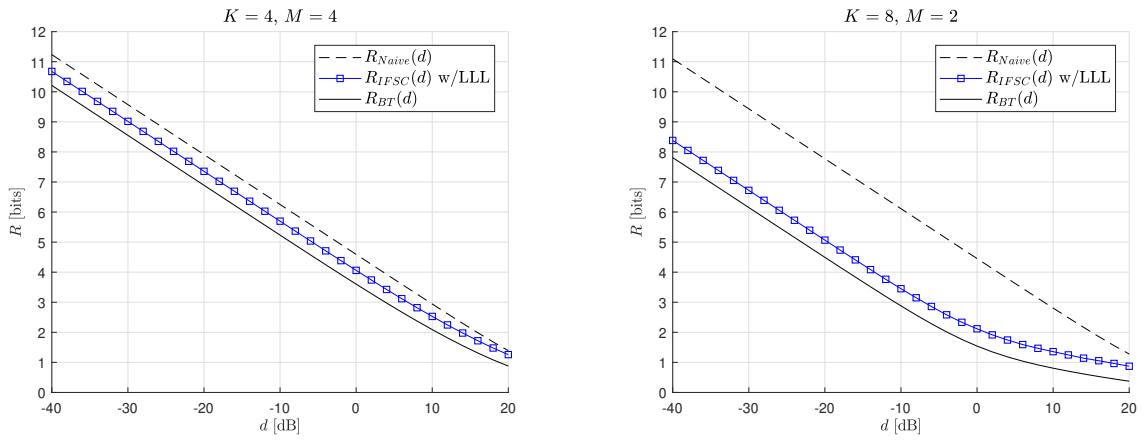
2.3.4 Replication of Results

With a setup for the correlation model for the the observations of the relays established, and having the rate-distortion expressions of the schemes used for comparison defined, it is now possible to obtain the rate-distortion curves for a set of predefined distortions. The rates given by (2.41), (2.52) and (2.53) for the IFSC scheme, the Berger-Tung scheme, and for the naive scheme respectively, were computed for a distortion interval of $[-40; 20]$ dB where the step between distortion values is 2 dB. For each of these distortion values a channel matrix $\mathbf{H}$, as specified in the previous section, is randomly generated and a covariance matrix $\mathbf{K_{xx}}$ is calculated with expression (2.51) to be used in the computation of the rates. Moreover, to obtain the results presented in this section, the process of randomly generating a channel matrix $\mathbf{H}$ and computing the corresponding covariance matrix $\mathbf{K_{xx}}$ is simulated 1000 times for each distortion. Each final rate presented for each distortion d is therefore an average of 1000 rates obtained for different $\mathbf{K_{xx}}$. This amounts to averaging the rates obtained with (2.41), (2.52), and (2.53) over 1000 different correlation scenarios with a target distorion d.

Two setups were considered as in [24], the setup with $K = 4$ relays and $M = 4$ transmitters, and the setup with $K = 8$ relays and $M = 2$ transmitters. For both setups a SNR of 20 dB was considered. The rate-distortion curves for the three coding schemes in these two setups are presented in figures 2.16(a) and 2.16(b). One should notice that both results fully match the ones presented in [24].

The first conclusion that can be drawn from this results is that there is a significant gap between the schemes that take advantage of the existing correlation between sources and the one that does not. This conclusion derives from examining the results for the setup with $K = 8$ and $M = 2$, having more relays than transmitters, which results in a higher correlation between the sources. In these results it is possible to see that both the IFSC scheme and the Berger-Tung scheme clearly outperform the naive scheme in terms of the necessary rate to obtain a certain target distortion d.

The second conclusion is that for both setups it is possible to see that $R_{IFSC}(d)$ follows the benchmark $R_{BT}(d)$ very closely with a gap of about half a bit for the target distortion interval considered. This raises the question of whether it is possible to reduce this gap with an alternative to the LLL algorithm that solves the SIVP and returns a "better" integer-valued full-rank matrix $\mathbf{A}$ such that $R_{IFSC}(d)$ is



(a) (b)

Figure 2.16: Integer-forcing source coding rate-distortion curves. The rate-distortion curve attained by the IFSC scheme, $R_{IFSC}(d)$, is compared with the one attained by the Berger-Tung scheme, $R_{BT}(d)$, and the one attained by the naive scheme, $R_{Naive}(d)$, for the setup with $K = M = 4$ (a) and for the setup with $K = 8$, $M = 2$ (b).

reduced. This is the motivation for the next chapter.

2.4 Closing Remarks

In this chapter the IFSC scheme that tackles the problem of distributed lossy compression was presented, closely following the recent proposal in [24]. The scheme provides a solution to the case where there exists a spatial correlation between the observations of K encoders but these are not allowed to exchange information between them. Instead, after a compression done at the encoders using a nested lattice codebook, the decoder estimates the source by means of a process that involves integer linear combinations of the incoming signals from the encoders. This decoding process depends on an underlying optimization problem that consists in finding an optimal integer-valued full-rank matrix $\mathbf{A}^*$ in order to reduce the necessary rate that attains a given target distortion. This optimization problem is, as mentioned in the previous sections, a shortest independent vector problem that in this first approach is approximately solved with the well-known LLL algorithm. Another approach to solve the SIVP is taken in the next chapter in order to cope with larger numbers of relays than the ones that the LLL-based solution can cope with, given that the LLL algorithms fails to find the best basis of a lattice when the number of dimensions is large.

The discussion in this chapter also opens the question of how to adapt this new framework to a scenario where there is a finite set of possible correlation models rather than only a fixed one. This question is of special interest to channels that can change over time affecting the spatial correlation presented by the sources, and this situation will be addressed in this work.

The nested lattice codebook used in this scheme, by construction, has dimension equal to n, the number of time realizations of each observation retrieved by each encoder. It was shown in this chapter that the IFSC scheme obtains a final MSE distortion that is equal or smaller than a target distortion

when n goes to infinity, i.e, the performance of this scheme improves with the number of samples that are transmitted. This may become a burden in terms of complexity for the encoders that have to quantize their observations onto this high-dimensional nested lattice pair and this procedure may be, by itself, a high complexity operation. To tackle this situation, it is suggested in [24] the use of a "one-shot" version of the IFSC scheme, where each time realization n is compressed using a 1-dimensional nested lattice pair at each encoder. This simpler version of the IFSC scheme that trades complexity with performance will also be studied in this thesis.

Chapter 3

Information-Theoretic Rate-Distortion of Integer-Forcing Source Coding

The question raised at the end of section 2.3.4 with respect to the underlying optimization problem required by the IFSC scheme is addressed in this chapter. First, a statement of this optimization problem is made with the aid of the previously discussed lattice theory. After that, a new alternative to the used LLL algorithm that returns an exact solution is explored to solve the problem. To conclude this chapter, the rate-distortion results using this alternative algorithm are obtained and compared with the previously obtained results.

3.1 Underlying Optimization Problem of the IFSC Scheme

As was introduced in chapter 2, successive decoding when using the IFSC scheme depends on an integer-valued full-rank matrix $\mathbf{A}$ to perform integer linear combinations between the signals received by the scheme's decoder. The choice of this matrix determines the rate-distortion vector attainable by the scheme, as was explained in the previous chapter, and therefore this matrix has to be chosen appropriately. The underlying optimization problem amounts to finding an optimal matrix $\mathbf{A}^*$ such that

$$\mathbf{A}^* = \underset{\substack{\mathbf{A}\in\mathbb{Z}^{K\times K}\\ \det(\mathbf{A})\neq 0}}{\arg\min} \left(\max_{k=1,\dots,K} \mathbf{a}_k^T (\mathbf{I} + \frac{\mathbf{K_{xx}}}{d}) \mathbf{a}_k \right). \tag{3.1}$$

Noting that $\mathbf{G} = (\mathbf{I} + \frac{\mathbf{K_{xx}}}{d})$ is a symmetric and positive definite Gram matrix, it admits a Cholesky decomposition given by

$$(\mathbf{I} + \frac{\mathbf{K_{xx}}}{d}) = \mathbf{G} = \mathbf{R}^T\mathbf{R}, \tag{3.2}$$

where $\mathbf{R} \in \mathbb{R}^{K\times K}$ is an upper triangular matrix, and therefore (3.1) can be updated to

$$\mathbf{A}^* = \underset{\substack{\mathbf{A}\in\mathbb{Z}^{K\times K}\\ \det(\mathbf{A})\neq 0}}{\arg\min} \left(\max_{k=1,\dots,K} \|\mathbf{R}\mathbf{a}_k\|^2 \right). \tag{3.3}$$

The upper triangular matrix $\mathbf{R}$ can be seen as the generator matrix of a K-dimensional lattice $\Lambda(\mathbf{R})$ and each vector $\mathbf{a}_k$ a vector that spans a specific lattice point of $\Lambda(\mathbf{R})$ through the multiplication by $\mathbf{R}$. To solve the problem expressed by (3.3) one has to find an interger-valued full-rank matrix $\mathbf{A}^* = [\mathbf{a}_1^*, ..., \mathbf{a}_K^*] \in \mathbb{Z}^{K\times K}$ such that $\max_{k=1,...,K} \|\mathbf{R}\mathbf{a}_k\|^2$ is as small as possible. This value is referred to as the Kth successive minimum of lattice $\Lambda(\mathbf{R})$, recalling the definition for a lattice's successive minima provided in section 2.2. Solving the problem at hand is then equivalent to solving a SIVP defined as finding an integer-valued full-rank matrix $\mathbf{A}^* \in \mathbb{Z}^{K\times K}$ such that

$$\max_{k=1,...,K} \|\mathbf{R}\mathbf{a}_k^*\| \leq \theta_K, \tag{3.4}$$

where θ_K is the Kth successive minimum of lattice $\Lambda(\mathbf{R})$. Furthermore, as stated in [39], it is advantageous to solve a successive minima problem (SMP) instead of the SIVP, even though they are both NP-hard. This SMP corresponds to finding an integer-valued full-rank matrix $\mathbf{A}^* \in \mathbb{Z}^{K\times K}$ such that

$$\|\mathbf{R}\mathbf{a}_k^*\| = \theta_k \text{ for } k = 1, ..., K, \tag{3.5}$$

with the θ_k defined as in chapter 2. The solution to this SMP also solves the SIVP and so an algorithm to solve the SMP is used in this thesis. A new algorithm has been recently proposed in [33] to solve this NP-hard problem, and it will be presented in the following section.

3.2 Solving the Successive Minima Problem

The recently proposed algorithm that will be used to solve the previoulsy presented SMP is explored in this section. Before tackling the SMP directly, this algorithm first uses a LLL reduction to preprocess the SMP. Specifically, the generator matrix $\mathbf{R}$ of the lattice of which one wants to find the K successive minima is first reduced using the LLL algorithm to obtain $\mathbf{R}_{red}$. $\mathbf{R}_{red}$ and $\mathbf{R}$ relate through expression (2.48) and generate the same lattice as mentioned in section 2.3.2. For the sake of efficiency of the algorithm, it is important that this reduced generator matrix is also an upper triangular matrix which is not the case after a LLL reduction. To guarantee that feature a QR decomposition is applied to $\mathbf{R}_{red}$ in order to obtain

$$\mathbf{R}_{red} = \bar{\mathbf{Q}}\bar{\mathbf{R}}, \tag{3.6}$$

where $\bar{\mathbf{Q}} \in \mathbb{R}^{K\times K}$ is an orthogonal matrix that when multiplied with $\bar{\mathbf{R}}$ amounts to rotating or reflecting the lattice generated by $\bar{\mathbf{R}}$, $\Lambda(\bar{\mathbf{R}})$, to obtain the lattice generated by $\mathbf{R}_{red}$, $\Lambda(\mathbf{R}_{red})$ [31].

The closest vector problem (CVP) is the one of finding the shortest lattice points closest to a given lattice point. Because in the CVP an initial target lattice point is given, this induces an absolute orientation in the geometry of the problem. The SIVP can be seen as a special case of the CVP, where the initial target lattice point is the origin, i.e., the zero vector, which has no particular direction. That is, the problem of finding linearly independent vectors in the lattice that are close to the origin becomes independent of any particular orientation of those successive minima. Hence, solving for the successive

minima of lattice $\Lambda(\mathbf{R}_{red})$, that is the same as solving the SIVP as previously stated, is equivalent to solving the successive minima of lattice $\Lambda(\bar{\mathbf{R}})$ that results from a rotation of $\Lambda(\mathbf{R}_{red})$. With this in mind, the SMP can be updated to a reduced SMP (RSMP) where one wants to find an integer-valued full-rank matrix $\mathbf{C}^* = [\mathbf{c}_1^*, ..., \mathbf{c}_K^*] \in \mathbb{Z}^{K \times K}$ such that

$$\|\mathbf{R}_{red}\mathbf{c}_k^*\| = \left\|\bar{\mathbf{R}}\mathbf{c}_k^*\right\| = \theta_k, \tag{3.7}$$

for $k = 1, ..., K$. Since expressions (3.5) and (3.7) are equivalent, one obtains

$$\begin{aligned} \|\mathbf{R}\mathbf{a}_k^*\|^2 &= \|\mathbf{R}_{red}\mathbf{c}_k^*\|^2 \\ \mathbf{R}\mathbf{a}_k^* &= \mathbf{R}_{red}\mathbf{c}_k^* \\ \mathbf{R}\mathbf{a}_k^* &= \mathbf{R}\mathbf{T}\mathbf{c}_k^* \\ \mathbf{a}_k^* &= \mathbf{T}\mathbf{c}_k^*, \end{aligned} \tag{3.8}$$

that yields the relationship between the solutions of the SMP and the RSMP

$$\mathbf{A}^* = \mathbf{T}\mathbf{C}^*, \tag{3.9}$$

where $\mathbf{T}$ is the unimodular matrix returned by the LLL algorithm. This first part of the algorithm can be summarized with the pseudocode provided in [33], here presented in Algorithm 1.

Algorithm 1 Algorithm to solve the SMP

Input: A symmetric and positive definite Gram matrix $\mathbf{G} \in \mathbb{R}^{K \times K}$.

Output: An optimal integer-valued full-rank matrix $\mathbf{A}^* \in \mathbb{Z}^{K \times K}$.

1. Perform a Cholesky decomposition to $\mathbf{G}$ to obtain the nonsingular upper triangular matrix $\mathbf{R}$.
2. Perform a LLL reduction to $\mathbf{R}$ to obtain $\mathbf{R}_{red}$ and the unimodular matrix $\mathbf{T}$.
3. Apply a QR decomposition to $\mathbf{R}_{red}$ to get the nonsingular upper triangular matrix $\bar{\mathbf{R}}$.
4. Input $\bar{\mathbf{R}}$ in Algorithm 2 to solve the RSMP and return $\mathbf{C}^*$.
5. Compute $\mathbf{A}^* = \mathbf{T}\mathbf{C}^*$.

After this problem reduction, the algorithm starts with a suboptimal matrix $\mathbf{C}$ that is updated throughout the algorithm until a solution to the RSMP is found. This update is made by finding new column vectors $\mathbf{c}_k$ such that at the end of the search procedure, $\mathbf{C}^*$ is an invertible integer-valued matrix and $\|\mathbf{c}_k^*\|$ are as short as possible, for $k = 1, ..., K$. To do so, an improved Schnorr-Euchner search algorithm proposed in [40] is used. Before introducing this improved version, the original Schnorr-Euchner tree search algorithm [41] to solve the Shortest vector Problem (SVP) given by

$$\mathbf{c}^* = \underset{\mathbf{c} \in \mathbb{Z}^{K \times 1} \setminus \{\mathbf{0}\}}{\arg\min} \left\|\bar{\mathbf{R}}\mathbf{c}\right\|^2 \tag{3.10}$$

is briefly explained. Assuming that $\mathbf{c}$ is within the hyper-ellipsoid defined by

$$\left\|\bar{\mathbf{R}}\mathbf{c}\right\|^2 < \beta^2 \tag{3.11}$$

where β is a constant. If one considers that

$$q_i = -\frac{1}{\bar{r}_{ii}} \sum_{j=i+1}^{K} \bar{r}_{ij} c_j \text{ for } i = K-1, ..., 1, \tag{3.12}$$

then (3.11) can be updated to

$$\sum_{i=1}^{K} \bar{r}_{ii}^2 (c_i - q_i)^2 < \beta^2 \tag{3.13}$$

which in turn is equivalent to

$$\bar{r}_{ii}^2 (c_i - q_i)^2 < \beta^2 - \sum_{j=i+1}^{K} \bar{r}_{jj}^2 (c_j - q_j)^2 \tag{3.14}$$

for $i = K-1, ..., 1$, where i is designated the level index. At level i in the search tree, this algorithm tries to choose a c_i that satisfies (3.14) when $c_K, c_{K-1}, ..., c_{i+1}$ have been chosen and $c_{i-1}, c_{i-2}, ..., c_1$ have not been chosen yet. The search procedure starts with $\beta = \infty$ and for $i = K, K-1, ..., 1$, q_i is computed through expression (3.12). Then one sets $c_i = \lfloor q_i \rceil$ where $\lfloor q_i \rceil$ rounds q_i to its nearest integer (in case of a tie q_i is rounded to the integer with the smaller magnitude), which implies $c_i = 0$ and inequality (3.14) holds. With this, $\mathbf{c} = \mathbf{0}$ is obtained but since $\mathbf{c}^* \neq \mathbf{0}$, $\mathbf{c}$ should be updated. To do so one sets c_1 as the next closest integer to q_1 and since there are two choices, one sets $c_1 = 1$. Since $\beta = \infty$, expression (3.14) with $i = 1$ holds for the updated $\mathbf{c}$, that is stored. Next, β is updated to $\beta = \left\|\bar{\mathbf{R}}\mathbf{c}\right\|$ in order to update $\mathbf{c}$ and find the optimal solution. Since the two sides of (3.14) with $i = 1$ are now equal, c_1 cannot be updated because this would increase the left side of the inequality and (3.14) would not hold. Thus, the algorithm moves on to level 2 to try to update c_2 as the next closest integer to q_2. If (3.14) with $i = 2$ holds, the algorithm jumps to $i = 1$ to update c_1 with a new computed q_1 via expression (3.12). If (3.14) with $i = 2$ does not hold, the algorithm jumps to $i = 3$ to try to update c_3 and so on. Finally, when it is not possible to update $\mathbf{c}$ such that (3.14) for $i = K$ holds, the search process terminates and the optimal $\mathbf{c}^*$ that satisfies (3.10) is returned.

The algorithm proposed in [33] to solve the previously stated RSMP shall be henceforth referred to as the successive minima (SM) algorithm. It starts with a suboptimal matrix $\mathbf{C}$ that corresponds to a $K \times K$ identity matrix with column permutations such that

$$\left\|\bar{\mathbf{R}}\mathbf{c}_1\right\| \leq \left\|\bar{\mathbf{R}}\mathbf{c}_2\right\| \leq \cdots \leq \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|, \tag{3.15}$$

holds. One now sets $\beta = \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|$, and a modified version of the previously described Schnorr-Euchner tree search algorithm is used to search nonzero integer vectors $\mathbf{c}$ that satisfy (3.11) to update $\mathbf{C}$. When $\mathbf{c} = \mathbf{0}$ is obtained, c_1 is set as the next closest integer to q_1 in order to get a nonzero integer vector $\mathbf{c}$ that satisfies $\left\|\bar{\mathbf{R}}\mathbf{c}\right\| \leq \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|$. This vector $\mathbf{c}$ is then used to update $\mathbf{C}$ as specified in [33] that in

this thesis is summarized by the pseudocode presented in Algorithm 3. Afterwards, one again sets $\beta = \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|$. It should be noted that β only decreases when the last column of $\mathbf{C}$ is changed after $\mathbf{C}$ is updated. Then, the algorithm proceeds by finding a new $\mathbf{c}$ to update $\mathbf{C}$ with the Schnorr-Euchner tree search algorithm. Finally, when $\mathbf{C}$ can no longer be updated and β cannot be decreased any further, the algorithm terminates and outputs the optimal integer-valed full-rank matrix $\mathbf{C}^*$ that is the solution to the RSMP.

The improvement made in [40] in respect to the Schnorr-Euchner tree search algorithm comes as a consequence of noting that if $\mathbf{c}$ is a solution to (3.10), then so is $-\mathbf{c}$. Hence, to speed up the search process, if $\mathbf{c}$ satisfies $\mathbf{c}_{i+1:K} = \mathbf{0}$ it is only necessary to search $c_i \geq 0$ at level i. The pseudocode for the just described algorithm to solve the RSMP is provided in [33] and presented in Algorithm 2 where

$$\text{sgn}(x) \;=\; \begin{cases} 1, & x \geq 0 \\ -1, & x < 0 \end{cases}. \tag{3.16}$$

Algorithm 2 Algorithm to solve the RSMP

Input: A nonsingular upper triangular matrix $\bar{\mathbf{R}} \in \mathbb{R}^{K\times K}$.

Output: A solution $\mathbf{C}^*$ to the RSMP.

1. Set the level index as $i = K$, the suboptimal matrix $\mathbf{C}$ as the $K \times K$ identity matrix with column permutations such that (3.15) holds, and $\beta = \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|$.
2. Set $c_i = \lfloor q_i \rceil$ where q_i is obtained through (3.12) and $s_i = \text{sgn}(q_i - c_i)$.
3. If (3.14) does not hold, then go to step 4. Else if $i > 1$, set $i = i - 1$ and go to step 2. Else, i.e., $i = 1$, go to step 5.
4. If $i = K$ set $\mathbf{C}^* = \mathbf{C}$ and terminate. Else, set $i = i + 1$ and go to step 6.
5. If $\mathbf{c} \neq \mathbf{0}$ use Algorithm 3 to update $\mathbf{C}$, set $\beta = \left\|\bar{\mathbf{R}}\mathbf{c}_K\right\|$ and $i = i + 1$.
6. If $i = K$ or $\mathbf{c}_{i+1:K} = \mathbf{0}$, set $c_i = c_i + 1$ and go to step 3. Else, set $c_i = c_i + s_i$, $s_i = -s_i - \text{sgn}(s_i)$ and go to step 3.

Algorithm 3 Algorithm to update $\mathbf{C}$

Input: A full column rank matrix $\mathbf{C} \in \mathbb{Z}^{K\times K}$, a nonzero column vector $\mathbf{c} \in \mathbb{Z}^{K\times 1}$ and a nonsingular upper triangular matrix $\bar{\mathbf{R}} \in \mathbb{R}^{K\times K}$.

Output: An invertible matrix $\bar{\mathbf{C}} \in \mathbb{Z}^{K\times K}$ whose columns are chosen from $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_K$ and $\mathbf{c}$ such that $\left\|\bar{\mathbf{R}}\bar{\mathbf{c}}_1\right\| \leq \left\|\bar{\mathbf{R}}\bar{\mathbf{c}}_2\right\| \leq \cdots \leq \left\|\bar{\mathbf{R}}\bar{\mathbf{c}}_K\right\|$ and $\left\|\bar{\mathbf{R}}\bar{\mathbf{c}}_k\right\|$ are as small as possible for all $1 \leq k \leq K$.

1. Find k and form $\tilde{\mathbf{C}} = [\mathbf{c}_1 \;\ldots\; \mathbf{c}_k \quad \mathbf{c} \quad \mathbf{c}_{k+1} \;\ldots\; \mathbf{c}_K]$ such that it satisfies $\left\|\bar{\mathbf{R}}\tilde{\mathbf{c}}_1\right\| \leq \cdots \leq \left\|\bar{\mathbf{R}}\tilde{\mathbf{c}}_{K+1}\right\|$.
2. Reduce $\tilde{\mathbf{C}}$ to its row echelon form by Gaussian elimination and denote it by $\mathbf{F}$ in order to efficiently find the index j of the column of $\tilde{\mathbf{C}}$ that is linearly dependent to $\tilde{\mathbf{c}}_i$ for some $1 \leq i \leq j - 1$.
3. Check if it exists a j such that $f_{jj} = 0$ for $j = k + 1, ..., K$. If it does, set $\bar{\mathbf{C}} = \tilde{\mathbf{C}}_{[\backslash j]}$. Otherwise if $f_{jj} \neq 0$ for all $k + 1 \leq j \leq K$, set $\bar{\mathbf{C}} = \tilde{\mathbf{C}}_{[\backslash (K+1)]}$.

3.3 Complexity of the Successive Minima Algorithm

The proof of the optimality of the previously described algorithm to solve the SMP is provided in [33] as well as an expression for the expected value of its complexity. In order to compare this complexity with the one of the previously used algorithm to solve the underlying optimization problem, the LLL algorithm, the $\mathcal{O}$-notation is used [42]. This notation is commonly used to describe the time complexity of an algorithm that tries to solve a problem of dimension N. In other words, it describes how the execution time required by an algorithm depends on that dimension N. The dimension of the optimization problem discussed in this thesis corresponds to K, the number of encoders in the IFSC scheme.

The complexity of the standard LLL algorithm used in this thesis is provided in [43] as $\mathcal{O}(K^4 \log K)$. The LLL algorithm is then of polynomial complexity in K, depending on the fourth power of K. The $\log K$ part is negligible since it grows very slowly with K. This polynomial running time of an algorithm that solves a NP-hard problem such as the optimization problem of IFSC was the main breakthrough introduced by the LLL algorithm.

Regarding the complexity of the discussed algorithm, since it depends on a tree search, the Schnorr-Euchner tree search algorithm, its complexity varies according to the visited number of nodes and, as a consequence, it does not have a fixed complexity. However, an expression for the expected value of this complexity can be obtained and is stated in [33] as

$$\mathbb{E}\big[C(K)\big] = \mathcal{O}\big(K^{\frac{5}{2}}(2\pi e)^{\frac{K}{2}}\big), \tag{3.17}$$

where $C(K)$ denotes the time complexity with respect to the dimension of the problem K. As expressed by (3.17), the SM algorithm has a polynomial part of order $\frac{5}{2}$ that, if isolated, would lead to a polynomial running time. However, due to the use of the tree search algorithm, it also has an exponential part that grows with $\frac{K}{2}$ which leads to an exponential overall running time of the SM algorithm.

In terms of complexity it is clear that the SM algorithm presents a higher complexity than the LLL algorithm since the former has an exponential running time, and the latter a polynomial running time as mentioned before. This does not come as a surprise since the SM algorithm itself incorporates a LLL reduction. Regarding the solution found by both algorithms, one can state that the SM algorithm finds an exact solution to the optimization problem according to the proof of optimality presented in [33]. The LLL-based approach returns an approximated solution to the optimization problem since it finds short lattice basis vectors that may not be the shortest ones, i.e., may not correspond to the successive minima. In the next section the gap between these two solutions is visualized by means of the rate-distortion curves attained by each solution.

3.4 Simulation of the Successive Minima Algorithm

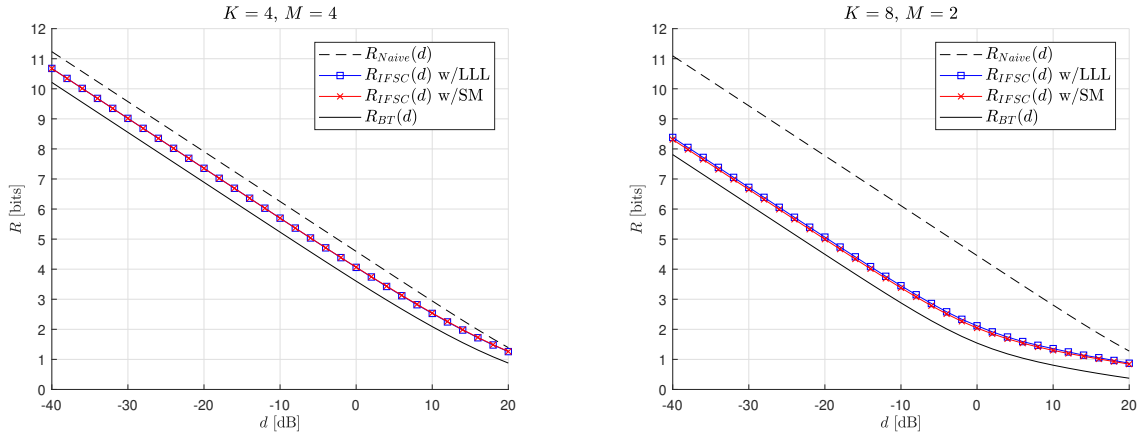
In order to compare the rates obtained when using the LLL algorithm to solve the underlying optimization problem of the IFSC scheme with the rate obtained when using the previously discussed algorithm to

solve that problem, the example of section 2.3.3 was used to provide a correlation model. For this example of compressing correlated encoder's observations in a Gaussian network, an expression for the covariance matrix is given by (2.51) considering a SNR of 20 dB and a channel matrix $\mathbf{H}$ with entries randomly generated from a Gaussian distribution $\mathcal{N}(0,1)$. As stated before, this covariance matrix, along with a given target distortion d, gives rise to the underlying optimization expressed by (3.1), which in these simulations was solved with the SM algorithm instead of the LLL algorithm. With the optimal integer-valued full-rank matrix $\mathbf{A}^*$ available, the rate $R_{IFSC}(d)$ can be computed through (2.41) for the given target distortion d. As with the previously presented simulations, a distortion interval of $[-40; 20]$ dB where the step between distortion values is 2 dB was considered, and for each one a different covariance matrix was computed 1000 times so that the final rate is an average of 1000 rate values obtained for different covariance matrices. Since the SM algorithm yields the exact solution to the underlying optimization problem, the rate-distortion curve $R_{IFSC}(d)$ obtained with this algorithm for any setup considered corresponds to the minimum rate required to obtain a maximum distortion d attainable with the IFSC scheme. For comparison, the rate-distortion curve for the IFSC scheme using the LLL algorithm was plotted, as well as the rate-distortion curves attained with the Berger-Tung scheme and with the naive scheme.

The first set of simulations were performed for the two setups considered in the previous chapter, the setup with $K = 4$ encoders and $M = 4$ transmitters, and the setup with $K = 8$ encoders and $M = 2$ transmitters. The rate-distortion curves obtained for each setup are respectively shown in figures 3.1(a) and 3.1(b). As it is possible to observe in these results, for the setup with $K = M = 4$ the rate-distortion curves obtained for the IFSC scheme using the SM algorithm and using the LLL algorithm match. From this it is possible to conclude that for $K = 4$, which is the dimension of the optimization problem, the LLL algorithm returns a solution that is optimal since it is equal to the one returned by the SM algorithm that, as said before, is an exact one. The same does not happen for the setup with $K = 8$, $M = 2$ where there is a very small performance gap between the two rate-distortion curves. This indicates that for an optimization problem of dimension $K = 8$, the solution returned by the LLL algorithm is, on average, an approximate one and not an exact one. However, since one has such a small performance gap between the two rate-distortion curves, one can state that the approximate solution returned by the LLL algorithm is a good approximation in this context.

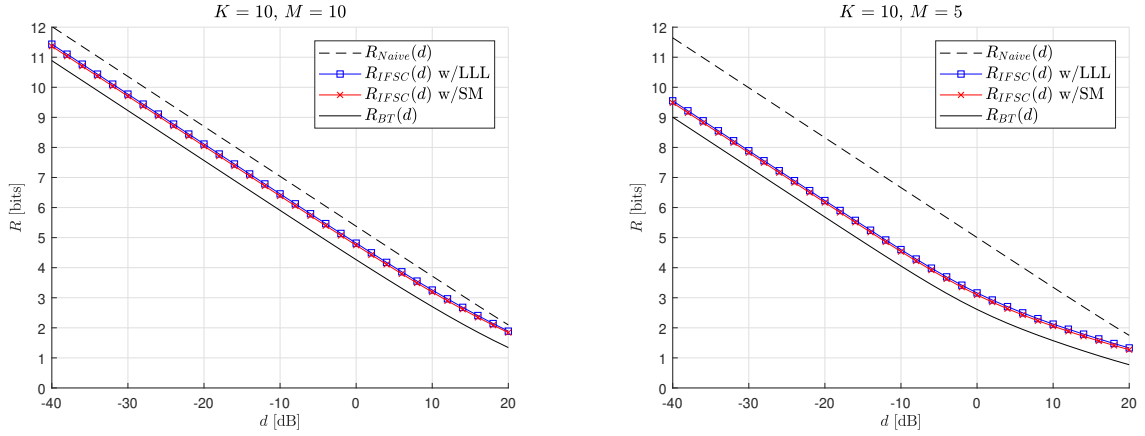
In order to assess how much this performance gap increases for increasing K, five more setups were simulated. In the first two setups, $K = 10$ was considered along with $M = 10$ and $M = 5$. The rate-distortion curves for these setups are presented in figure 3.2 and it is possible to observe that there is also a very small performance gap between the two rate-distortion curves for the IFSC scheme. Comparing this performance gap with the one obtained for the setup with $K = 8$, $M = 2$, one can state that these are very similar which indicates that the approximate solution to the optimization problem returned by the LLL algorithm for this value of K is also a good approximation to the exact one.

For the second pair of setups simulated, K and M were doubled to obtain a setup with $K = M = 20$ and another one with $K = 20$, $M = 10$. For these setups, the performance gap obtained is now quite visible in figure 3.3, denoting that the solution returned by the LLL algorithm no longer is a good



(a) (b)

Figure 3.1: Integer-forcing source coding rate-distortion curves with the SM algorithm for the setups $K = M = 4$ (a) and $K = 8$, $M = 2$ (b).



(a) (b)

Figure 3.2: Integer-forcing source coding rate-distortion curves with the SM algorithm for the setups $K = 10$, $M = 10$ (a) and $K = 10$, $M = 5$ (b).

approximation of the exact one that is found by the SM algorithm.

Finally, for the setup with $K = M = 25$ this trend of increasing performance gap for increasing K is also verified by examining figure 3.4. This reinforces the fact that for an increase of the dimension of the underlying optimization problem, which is done by increasing the number of encoders in the IFSC scheme, the approximate solution found by the LLL algorithm becomes a poor approximation of the exact solution. An important conclusion is that there is a degradation in performance with respect to the optimum attainable rate for a given target distortion d for increasing K when using the LLL algorithm in the IFSC scheme.

To further compare the two algorithms used to solve the optimization problem, the approximated running times of each algorithm for the dimensions of the problem simulated in this section are presented in Tables 3.1 and 3.2. These running times correspond to the approximated time each algorithm takes to find the solution to the optimization problem for a given covariance matrix $\mathbf{K_{xx}}$ and a distortion d, in a scenario with K encoders. As expected after the previous analysis regarding the complexity of

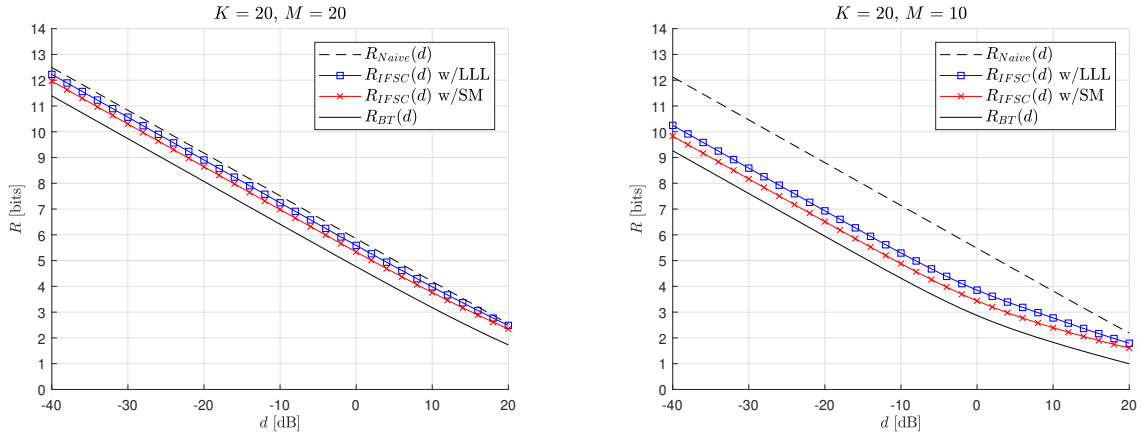


Figure 3.3: Integer-forcing source coding rate-distortion curves with the SM algorithm for the setups $K = 20$, $M = 20$ (a) and $K = 20$, $M = 10$ (b).

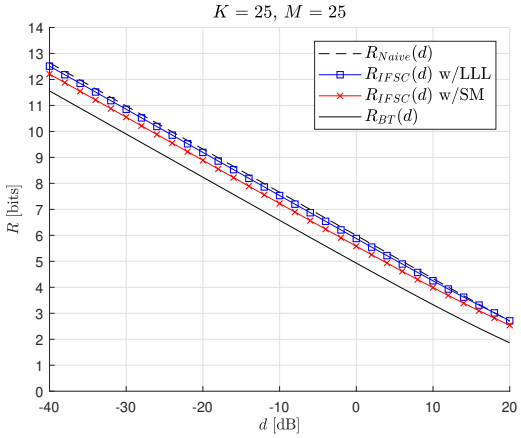


Figure 3.4: Integer-forcing source coding rate-distortion curves with the SM algorithm for the setup $K = M = 25$.

each algorithm, the approximated running time for every K is smaller when the LLL algorithm is used. Moreover, for increasing K it is possible to observe that the gap between running times attained by the two algortithms also increases. These particular simulations were performed with Matlab 2017b on a computer with Intel(R) Core(TM) CPU i5-2450M working at 2.4 GHz.

Dimension of the problem K	**Approx. running time**
4	80 ms
8	150 ms
10	200 ms
20	700 ms
25	2 s

Table 3.1: Approximated running time of the LLL algorithm for the simulated values of K.

Dimension of the problem K	Approx. running time
4	300 ms
8	500 ms
10	800 ms
20	8 s
25	65 s

Table 3.2: Approximated running time of the SM algorithm for the simulated values of K.

3.5 Closing Remarks

In this chapter, a new algorithm to return an exact solution to the optimization problem introduced in chapter 2 was presented. Instead of directly approaching the SIVP, this algorithm solves the SMP that, as stated, also solves the SIVP. Further, for the sake of efficiency the algorithm first reduces the SMP to a RSMP with a LLL reduction and solves it using an improved Schnorr-Euchner tree search algorithm. When the search for the successive minima terminates, the algorithm returns an integer-valued full-rank matrix $\mathbf{C}^*$ that is the solution to the RSMP. This solution relates to the solution to the SMP through an unimodular matrix returned by the LLL lattice reduction and so $\mathbf{A}^*$ is obtained. This integer-vaued full-rank matrix $\mathbf{A}^*$ represents the exact solution to the optimization problem in the IFSC scheme context and so it is possible to obtain the information-theoretic minimum rate-distortion curves for this scheme.

If one increases the dimension of the optimization problem, which is equivalent to increase the number of encoders in the IFSC scheme, the gap between the solution returned by the LLL algorithm and the solution returned by the SM algorithm, that is the exact one, also increases as was pointed out in the previous chapter. This is mainly due to the fact that the LLL is an algorithm to perform lattice reduction and not an algorithm specifically designed to solve the SIVP, and so the solution it returns is only an approximate one.

Besides the performance gap, there is also a significant complexity difference between the two algorithms that favours the LLL algorithm, as mentioned in section 3.3. This leads to a trade-off between performance and complexity when deciding which algorithm to use in the IFSC scheme. For example if one considers a setup with $K = 8$ encoders, the complexity burden imposed on the decoder by the SM algorithm to attain the exact solution may not be worth affording since the solution attained by the LLL algorithm, which has a polynomial running time, is very close to the exact one. If processing power is not an issue for the decoder and a setup with $K = 20$ is considered, then the use of the SM algorithm is advantageous because with that number of dimensions there is a considerable performance gap between the two solutions.

Chapter 4

Semi-Blind Correlation Model

In the previous chapters the IFSC scheme assumes a fixed correlation model between the observations of the relays. This chapter extends IFSC to the case of having a finite set of possible correlations between the observations, corresponding to different scenarios that happen with some known probabilities. This new framework is initially described and then a solution is proposed. Finally, the simulation results are presented and analysed.

4.1 Problem Statement

As presented in chapter 2, the IFSC scheme explores the correlation model that exists between the observations of the encoders represented by a *fixed* covariance matrix $\mathbf{K_{xx}}$ that is known by the decoder. With this knowledge, the decoder computes an optimal matrix $\mathbf{A}^*$ by solving the optimization problem set by (3.1) that depends on $\mathbf{K_{xx}}$ to perform linear combinations between the signals it receives from the K encoders. It then uses those linear combinations to estimate the original sources with a final MSE smaller or equal than a given target distortion d, as specified in section 2.3.1.

The correlation model that is described by the covariance matrix $\mathbf{K_{xx}}$ can change over time and from situation to situation. Different factors may lead to this variation. One example is that of some sensors in a distributed sensor network that start to collect data that, for some reason, is not correlated to the data collected by the other sensors in that same network, thereby changing this correlation model. Another example is that of an extra device (e.g., a jammer) being placed near the network and corrupting the data collected by all sensors, consequently changing the correlation model. Shadowing can also play a role in this correlation model variation along with many other factors that are outside of the scope of this thesis. This variation creates the problem of selecting which correlation model best represents the correlation between the sources at a given point in time. To tackle this problem, one first considers the binary case where two covariance matrices that describe two different correlation models are possible. These covariance matrices are denoted by $\mathbf{K_{xx}^A}$ and $\mathbf{K_{xx}^B}$ and are both known by the decoder beforehand, which remains "blind" to which of these matrices best describes the correlation model for a given point in time.

$\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}}$ and $\mathbf{K}_{\mathbf{xx}}^{\mathbf{B}}$, as seen is section 2.3.2, lead to Gram matrices denoted here by $\mathbf{G_A}$ and $\mathbf{G_B}$ that in turn allow a Cholesky decomposition such that

$$\mathbf{G_A} = \mathbf{R_A}^T \mathbf{R_A}, \tag{4.1}$$

and

$$\mathbf{G_B} = \mathbf{R_B}^T \mathbf{R_B}. \tag{4.2}$$

$\mathbf{R_A}$ and $\mathbf{R_B}$ are generator matrices for the lattices $\Lambda(\mathbf{R_A})$ and $\Lambda(\mathbf{R_B})$, respectively. An example of these two different lattices is depicted in figure 4.1.

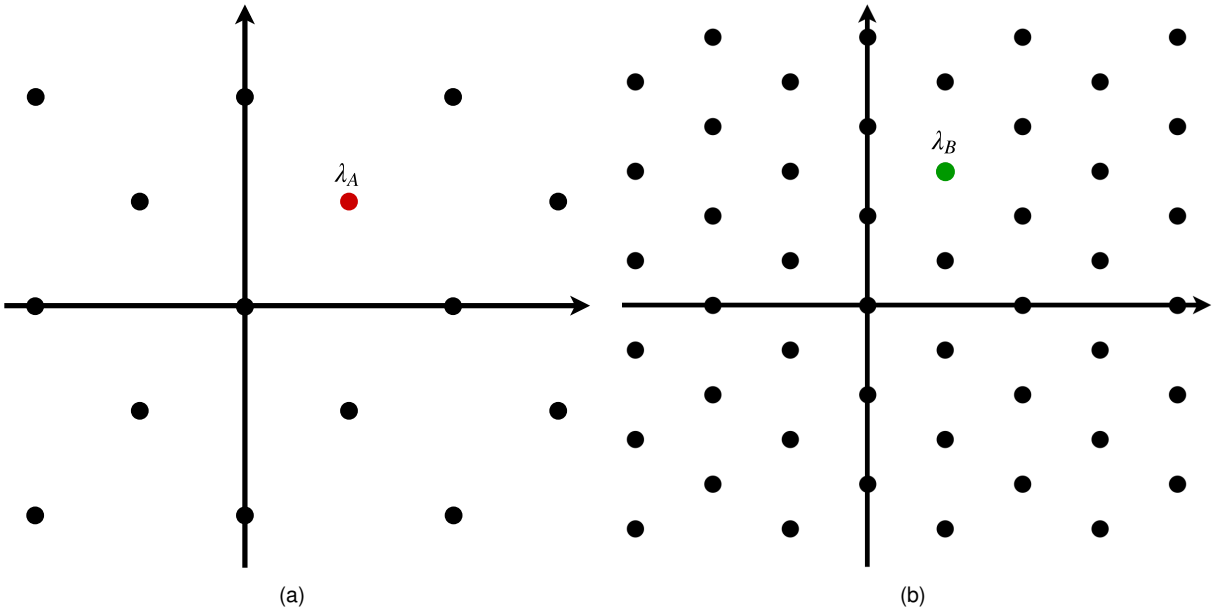


Figure 4.1: 2-dimensional lattices $\Lambda(\mathbf{R_A})$ (a) and $\Lambda(\mathbf{R_B})$ (b). Optimal matrix $\mathbf{A}_{\mathbf{A}}^*$ spans the lattice's linearly independent points closest to the origin of the lattice represented in (a) such as the lattice point λ_A highlighted in red. This same optimal matrix $\mathbf{A}_{\mathbf{A}}^*$ may not span the lattice's linearly independent points closest to the origin of the lattice represented in (b), and instead give rise to a lattice point λ_B highlighted in green.

By having two possible covariance matrices to describe the correlation model between the sources, the problem that arises is the one of deciding which matrix $\mathbf{A}^*$ should be computed. If this computation is performed with the optimal matrix $\mathbf{A}_{\mathbf{A}}^*$ obtained for $\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}}$, this does not guarantee that the same optimal matrix $\mathbf{A}_{\mathbf{A}}^*$ also spans the lattice's linearly independent points closest to the origin of a lattice $\Lambda(\mathbf{R_B})$. This problem is also exemplified in figure 4.1. To address this problem a proposed solution is presented in the following section.

4.2 Proposed Solution

One starts by assuming two different possible scenarios that give rise to two possible correlation matrices, $\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}}$ and $\mathbf{K}_{\mathbf{xx}}^{\mathbf{B}}$, with probabilities:

$$P(\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}}) = p \tag{4.3}$$

and

$$P(\mathbf{K_{xx}^B}) = 1 - p \tag{4.4}$$

for some $p \in [0; 1]$. For a random variable δ that follows a Bernoulli distribution, i.e., that takes the value 1 with probability p and takes value 0 with probability $1 - p$, a covariance matrix is selected at a given time slot according to

$$\tilde{\mathbf{K}}_{\mathbf{xx}} = \delta \mathbf{K_{xx}^A} + (1 - \delta)\mathbf{K_{xx}^B}. \tag{4.5}$$

This means that $\tilde{\mathbf{K}}_{\mathbf{xx}}$ is equal to either $\mathbf{K_{xx}^A}$ or to $\mathbf{K_{xx}^B}$ depending on the random binary variable δ. If $\mathbf{K_{xx}^A}$ is more likely than $\mathbf{K_{xx}^B}$ (p is greater than $1 - p$) then $\tilde{\mathbf{K}}_{\mathbf{xx}}$ is more likely to be equal to $\mathbf{K_{xx}^A}$, and, reciprocally, if $\mathbf{K_{xx}^B}$ is more likely than $\mathbf{K_{xx}^A}$. It is with this selected covariance matrix $\tilde{\mathbf{K}}_{\mathbf{xx}}$ that the rate $R_{IFSC}(d)$ attained by the IFSC scheme for a given target distortion d given by (2.41) is computed. The optimal matrix $\mathbf{A}^*$ is not obtained considering $\mathbf{R_A}$ or $\mathbf{R_B}$, but rather an extended generator matrix $\mathbf{R_{ext}} \in \mathbb{R}^{2K \times K}$ constructed by stacking the two in the following manner:

$$\mathbf{R_{ext}} = \begin{bmatrix} \sqrt{p}\,\mathbf{R_A} \\ - - - \\ \sqrt{1-p}\,\mathbf{R_B} \end{bmatrix}_{2K \times K}. \tag{4.6}$$

This concatenation creates another lattice generating matrix that, when searching for the shortest vectors of the lattice it spans, it takes into account, in different sets of sub-dimensions, the two constituting lattice generating matrices "weighted" by the probability of the respective scenario.

With this extended generator matrix, the problem at hand translates to minimizing

$$\max_{k=1,\ldots,K} \left\|\mathbf{y}_k^{ext}\right\|^2 = \max_{k=1,\ldots,K} \|\mathbf{R_{ext}}\mathbf{a}_k\|^2, \tag{4.7}$$

where $\mathbf{y}_k^{ext}$ for $k = 1, ..., K$ are K vectors that, when spanned by $\mathbf{A_{ext}^*}$, are the K linearly independent shortest vectors of $\Lambda(\mathbf{R_{ext}})$. The K column vectors $\mathbf{y}_k^{ext}$ form the $2K \times K$ matrix $\mathbf{Y_{ext}}$ that is given by

$$\mathbf{Y_{ext}} = \mathbf{R_{ext}}\mathbf{A_{ext}^*}. \tag{4.8}$$

Since $\mathbf{R_{ext}}$ is a concatenation of $\sqrt{p}\,\mathbf{R_A}$ and $\sqrt{1-p}\,\mathbf{R_B}$, one can write

$$\begin{gathered} \mathbf{y}_k^{ext} = \mathbf{R_{ext}}\mathbf{a}_k^{*ext} \\ \Leftrightarrow \\ \begin{bmatrix} y_1^{ext} \\ \vdots \\ y_{2K}^{ext} \end{bmatrix} = \begin{bmatrix} \sqrt{p}\,\mathbf{R_A} \\ - - - \\ \sqrt{1-p}\,\mathbf{R_B} \end{bmatrix} \begin{bmatrix} a_1^{*ext} \\ \vdots \\ a_K^{*ext} \end{bmatrix}. \end{gathered} \tag{4.9}$$

If one considers $\mathbf{y}_k^A$ for $k = 1, ..., K$ to be the K linearly independent shortest vectors of lattice $\Lambda(\mathbf{R_A})$ and $\mathbf{y}_k^B$ for $k = 1, ..., K$ to be the K linearly independent shortest vectors of lattice $\Lambda(\mathbf{R_B})$, one can write

that $\mathbf{y}_k^{ext}$ follows

$$\left\|\mathbf{y}_k^{ext}\right\|^2 = p\left\|\mathbf{y}_k^A\right\|^2 + (1-p)\left\|\mathbf{y}_k^B\right\|^2, \text{ for } k = 1, ..., K. \tag{4.10}$$

Setting $p = 1$, one has that the first K rows of $\mathbf{y}_k^{ext}$ correspond to $\mathbf{y}_k^A$, and $\mathbf{A}_{\mathbf{ext}}^*$ is equal to $\mathbf{A}_{\mathbf{A}}^*$. Further, setting $p = 0$, the last K rows of $\mathbf{y}_k^{ext}$ correspond to $\mathbf{y}_k^B$ and $\mathbf{A}_{\mathbf{ext}}^*$ is equal to $\mathbf{A}_{\mathbf{B}}^*$. With a value of p between 0 and 1 an optimal integer-valued full-rank matrix $\mathbf{A}_{\mathbf{ext}}^*$ is obtained that creates a compromise between the two possible correlations according to their individual probabilities.

An important feature of this proposed solution is that the obtained $\mathbf{A}_{\mathbf{ext}}^*$ is always a $K \times K$ matrix. This results from the fact that even though $\mathbf{R}_{\mathbf{ext}}$ is a $2K \times K$ matrix (for this binary case), it generates a K-dimensional lattice since there are only K generating vectors (in the columns of $\mathbf{R}_{\mathbf{ext}}$), even though they "live" in a $2K$ dimensional space. Moreover, $\mathbf{R}_{\mathbf{ext}}$ can be decomposed using a QR decomposition to obtain

$$\mathbf{R}_{\mathbf{ext}} = \bar{\mathbf{Q}}\bar{\mathbf{R}} \tag{4.11}$$

where $\bar{\mathbf{Q}}$ is a $2K \times 2K$ orthogonal matrix and $\bar{\mathbf{R}}$ is a $2K \times K$ matrix. The effect of $\bar{\mathbf{Q}}$ amounts to rotating or reflecting the lattice generated by $\bar{\mathbf{R}}$, $\Lambda(\bar{\mathbf{R}})$, to obtain the lattice generated by $\mathbf{R}_{\mathbf{ext}}$, $\Lambda(\mathbf{R}_{\mathbf{ext}})$. Because $\mathbf{R}_{\mathbf{ext}}$ has rank K, i.e., it has K linearly independent columns, $\bar{\mathbf{R}}$ is of the form

$$\bar{\mathbf{R}} = \begin{bmatrix} \bar{\mathbf{R}}' \\ --- \\ \mathbf{0} \end{bmatrix}, \tag{4.12}$$

where $\bar{\mathbf{R}}'$ is a $K \times K$ upper triangular matrix and $\mathbf{0}$ is a $K \times K$ zero matrix. Consequently, $\mathbf{R}_{\mathbf{ext}}$ can also be expressed as

$$\mathbf{R}_{\mathbf{ext}} = \bar{\mathbf{Q}}'\bar{\mathbf{R}}' \tag{4.13}$$

where $\bar{\mathbf{Q}}'$ is a $2K \times K$ orthogonal matrix that corresponds to the first K columns of $\bar{\mathbf{Q}}$. Expression (4.13) can be referred to as an "economy" QR decomposition of $\mathbf{R}_{\mathbf{ext}}$ since it only considers the first K columns of $\bar{\mathbf{Q}}$ and the first K rows of $\bar{\mathbf{R}}'$, ignoring the remaining ones. As before, the mutiplication of $\bar{\mathbf{R}}'$ by $\bar{\mathbf{Q}}'$ amounts to rotating or reflecting the lattice generated by $\bar{\mathbf{R}}'$, $\Lambda(\bar{\mathbf{R}}')$, to obtain the lattice generated by $\mathbf{R}_{\mathbf{ext}}$, $\Lambda(\mathbf{R}_{\mathbf{ext}})$.

As was justified in chapter 3, solving for the successive minima of lattice $\Lambda(\mathbf{R}_{\mathbf{ext}})$ is the same as solving for the successive minima of lattice $\bar{\mathbf{R}}'$ and so, no matter the number of possible covariance matrices to describe the correlation model in the IFSC scheme, the underlying optimization problem of finding $\mathbf{A}_{\mathbf{ext}}^*$ is always solved on a K-dimensional lattice. This is of great advantage in terms of the complexity burden imposed on the decoder to solve this optimization problem, which remains unchanged when the set of possible covariance matrices increases.

Given this nice feature of the extended problem, it is now possible to generalize beyond the binary case of two possible covariance matrices. Considering a set of N possible covariance matrices, these follow

$$\sum_{i=1}^{N} P(\mathbf{K}_{\mathbf{xx}}^{\mathbf{i}}) = 1 \tag{4.14}$$

and

$$P(\mathbf{K_{xx}^i}) = p_i \tag{4.15}$$

for $i = 1, ..., N$ and $p_i \in [0; 1]$. The selected covariance matrix for which the rate is calculated is now given by

$$\tilde{\mathbf{K}}_{\mathbf{xx}} = \delta_1 \mathbf{K_{xx}^1} + ... + \delta_N \mathbf{K_{xx}^N}, \tag{4.16}$$

where δ_i takes value 1 with probability p_i and 0 with probability $1 - p_i$ for $i = 1, ..., N$. Note that these Bernoulli random variables are restricted by $\delta_1 + ... + \delta_N = 1$. The extended lattice generator matrix $\mathbf{R_{ext}}$ is defined as

$$\mathbf{R_{ext}} = \begin{bmatrix} \sqrt{p_1}\,\mathbf{R_1} \\ - - - \\ \vdots \\ - - - \\ \sqrt{p_N}\,\mathbf{R_N} \end{bmatrix}_{NK \times K}, \tag{4.17}$$

where $\mathbf{R}_1, ..., \mathbf{R}_N$ are the lattice generator matrices that result from each corresponding covariance matrix $\mathbf{K_{xx}^1}, ..., \mathbf{K_{xx}^N}$. For a situation with three possible covariance matrices the row dimension of $\mathbf{R_{ext}}$ is $3K$, for four is $4K$ and so on for increasing N. This linear increase in the dimension of the extended generator matrix, as stated before, does not represent an increase in the computational burden since the problem is always reduced to a problem of finding the K successive minima of a lattice generated by a $K \times K$ matrix obtained through the "economy" QR decomposition of $\mathbf{R_{ext}}$. This "economy" QR decomposition yields

$$\mathbf{R_{ext}} = \bar{\mathbf{Q}}' \bar{\mathbf{R}}', \tag{4.18}$$

where $\bar{\mathbf{Q}}'$ is a $NK \times K$ orthogonal matrix and $\bar{\mathbf{R}}'$ a $K \times K$ upper triangular matrix that is used to solve the optimization problem finding the optimal integer-valued full-rank $K \times K$ matrix $\mathbf{A_{ext}^*}$.

In the following section the results of the simulation of this proposed solution are presented.

4.3 Simulation of the Proposed Solution

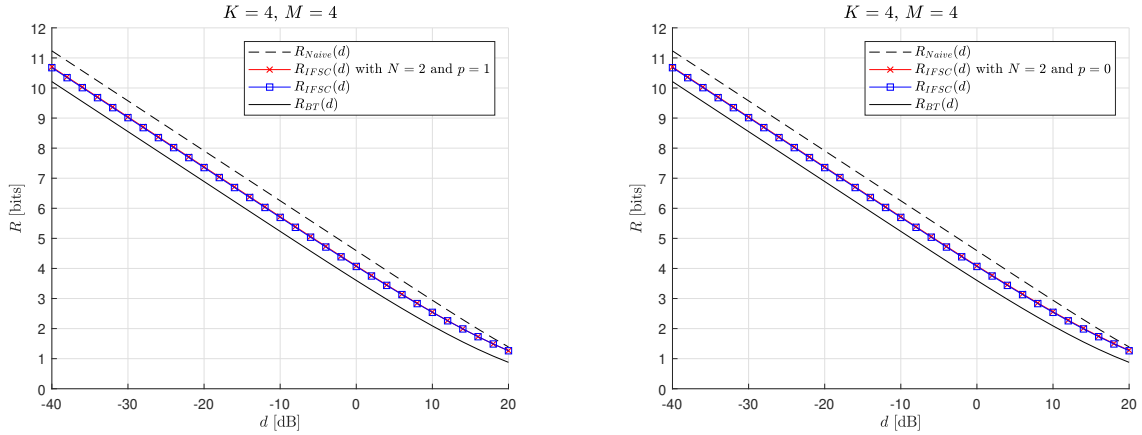
As in other simulations presented in this thesis, the example used to simulate the previously exposed proposed solution to approach the semi-blind correlation model problem is the same as used in section 2.3.3. With this example of compressing correlated encoder's observations in a Gaussian network, an expression for the covariance matrix that describes the correlation model between the encoders is provided and given by equation (2.51) considering a SNR of 20 dB. This time however, instead of randomly generating only a channel matrix $\mathbf{H}$ that would lead to a covariance matrix $\mathbf{K_{xx}}$, N channel matrices were randomly generated to compute N different possible covariance matrices. Each of these N possible covariance matrices had a probability associated with it that was changed from simulation to simulation. After that, the process described in the previous section was computed to obtain an optimal integer-valued full-rank matrix $\mathbf{A_{ext}^*}$. It is important to note that the algorithm used to solve

this optimization problem was the one specified in chapter 3, the SM algorithm, since it is the one that yields the exact solution. To conclude the process, the rate for the IFSC scheme was obtained through expression (2.41) for the selected covariance matrix $\tilde{\mathbf{K}}_{\mathbf{xx}}$, the optimal matrix $\mathbf{A}^*_{\mathbf{ext}}$ and the given target distortion d. As before, this was performed for each target distortion 1000 times so that the final rate corresponds to an average of 1000 rates.

The size of the sets of possible covariance matrices considered in the simulations were $N = 2$ (the binary case) and $N = 3$ for different pairs of K encoders and M transmitters. These simulations are compared to the previously obtained results for this setup with the IFSC scheme using the SM algorithm, the Berger-Tung scheme and the naive scheme, where only a single possible covariance matrix was considered in each of the 1000 simulations for each target distortion d.

4.3.1 $N = 2$ Possible Covariance Matrices

In this scenario, the two possible covariance matrices $\mathbf{K}^{\mathbf{A}}_{\mathbf{xx}}$ and $\mathbf{K}^{\mathbf{B}}_{\mathbf{xx}}$ have a probability $P(\mathbf{K}^{\mathbf{A}}_{\mathbf{xx}}) = p$ and $P(\mathbf{K}^{\mathbf{B}}_{\mathbf{xx}}) = 1 - p$ as stated before. One starts with the configuration with $K = 4$ encoders and $M = 4$ transmitters where the first simulations were obtained considering $p = 1$ and $p = 0$. These two cases are equivalent to finding an optimal matrix $\mathbf{A}^*_{\mathbf{ext}}$ equal to $\mathbf{A}^*_{\mathbf{A}}$ and to $\mathbf{A}^*_{\mathbf{B}}$, respectively. Hence, the rate-distortion curve obtained should match the one obtained considering only one covariance matrix for the IFSC scheme. This validated in figures 4.2(a) and 4.2(b), which present the simulation results for these two cases.

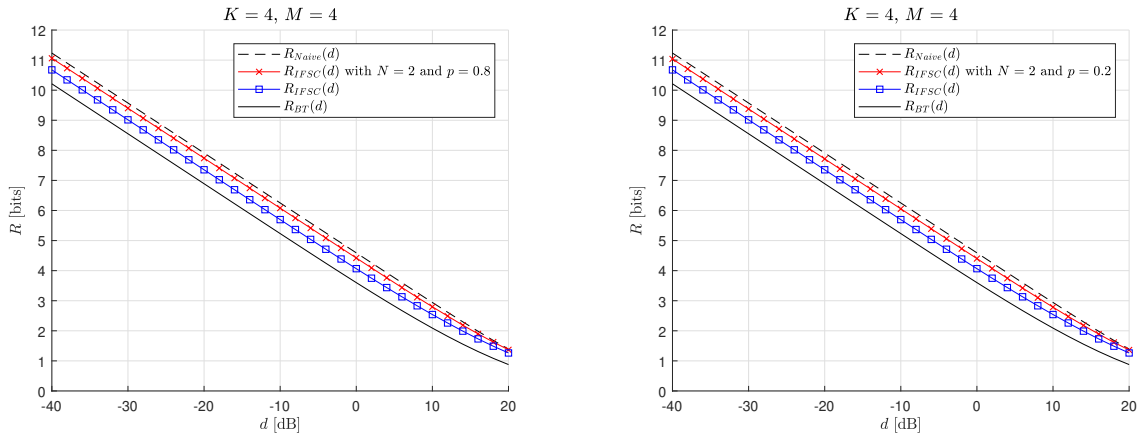


(a) (b)

Figure 4.2: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 1$ and $p = 0$ in the setup $K = M = 4$. With $p = 1$ (a) and $p = 0$ (b) the rate-distortion curve matches the one considering a single covariance matrix for the IFSC scheme.

The second set of simulations was performed considering that $p = 0.8$ and $p = 0.2$. For $p = 0.8$, $\mathbf{K}^{\mathbf{A}}_{\mathbf{xx}}$ is more likely to be the selected covariance matrix and $\mathbf{R}_{\mathbf{A}}$ has a higher contribution in the extended generator matrix $\mathbf{R}_{\mathbf{ext}}$, so the the computed optimal matrix $\mathbf{A}^*_{\mathbf{ext}}$ is more appropriate to the scenario described by $\mathbf{K}^{\mathbf{A}}_{\mathbf{xx}}$ than to the one described by $\mathbf{K}^{\mathbf{B}}_{\mathbf{xx}}$. The opposite happens when $p = 0.2$. The scheme is not adjusted to only one covariance matrix and makes a compromise between the two available covariance matrices. This compromise is not optimal for each individual situation and so the performance

was expected to be worse than the one considering a single covariance matrix. This is confirmed by the results obtained for the two cases in figures 4.3(a) and 4.3(b).



(a) (b)

Figure 4.3: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.8$ and $p = 0.2$ in the setup $K = M = 4$. With $p = 0.8$ (a) and $p = 0.2$ (b) the rate-distortion curve is above the one considering a single covariance matrix for the IFSC scheme indicating a worse performance but is below the rate-distortion curve for the naive scheme, outperforming it. These two cases are symmetric.

These results for $p = 0.8$ and $p = 0.2$ are identical, which denotes a symmetry that comes from the fact that both covariance matrices are obtained through the same expression (2.51), even though with different channel matrices $\mathbf{H}$. From these particular results one can conclude that using this proposed solution to approach the uncertainty regarding which covariance matrix best describes the correlation model returns a better overall performance than using the naive scheme, which does not take into consideration the correlation between the sources. This can be concluded from the fact that for $p = 0.8$ and $p = 0.2$ the rate-distortion curve obtained is below the one obtained for the naive scheme, $R_{Naive}(d)$.

When simulating with $p = 0.5$, the SM algorithm finds a matrix $\mathbf{A}^*_{\mathbf{ext}}$ that is neither optimal nor better for one covariance matrix in particular. Therefore, the rate-distortion curve obtained shows the worst performance among all values of p. In fact, with this choice of p, the rate-distortion curve attained matches the one obtained with the naive scheme, $R_{Naive}(d)$, as observed in figure 4.4.

The next setup considered was the one with $K = 8$ encoders and $M = 2$ transmitters, and one can again confirm that for $p = 1$ and $p = 0$, the rate-distortion curve obtained matches the one obtained considering only a single possible covariance matrix with the IFSC scheme as depicted in figures 4.5(a) and 4.5(b). For $p = 0.8$ and $p = 0.2$ the previously observed symmetry is conserved, and the proposed solution still outperforms the naive scheme as observed in figures 4.6(a) and 4.6(b). This meets what would be expected since the gap between the performance of the IFSC scheme and the naive scheme is larger for this setup than for the setup with $K = M = 4$ due to the fact that, with more relays and fewer sources, there exists more correlation between the observations of the encoders.

This larger gap between the IFSC and naive schemes introduces an interesting result when considering $p = 0.5$. Even though this probability distribution amounts to the worst performance among all values for p, it still leads to a rate-distortion curve below the one obtained with the naive scheme as observed

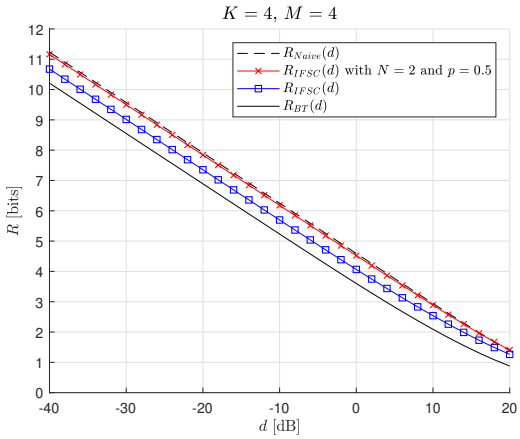
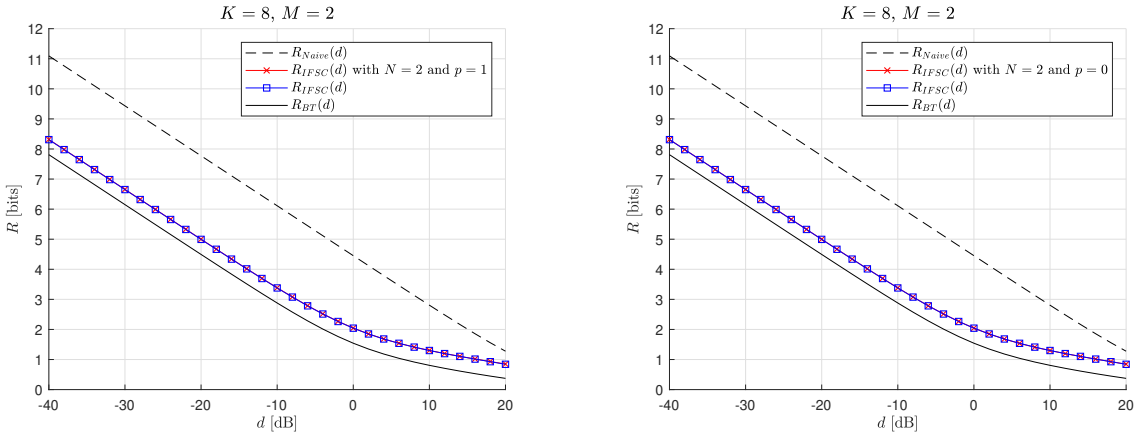


Figure 4.4: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.5$ in the setup $K = M = 4$. With $p = 0.5$ the rate-distortion curve matches the one considering a single covariance matrix for the naive scheme.



(a) (b)

Figure 4.5: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 1$ and $p = 0$ in the setup $K = 8$ and $M = 2$. With $p = 1$ (a) and $p = 0$ (b) the rate-distortion curve matches the one considering a single covariance matrix for the IFSC scheme.

in figure 4.7, which indicates a better performance. To further assess this situation another two setups with $K > M$ were simulated. In the first setup, the number of encoders was considered to be $K = 20$ and the number of transmitters $M = 10$. As it is possible to observe in figure 4.8(a), the rate-distortion curve for the IFSC scheme with the proposed approach and $p = 0.5$ is below the curve obtained with the naive scheme, indicating a better performance when the correlation is taken in consideration. Increasing even more the correlation between the encoder's observations by considering the setup of $K = 20$ encoders and $M = 2$ transmitters, the gap between these two curves is even larger as observed in figure 4.8(b). One can conclude from these results that even with total uncertainty about which of the two covariance matrices best describes the correlation model between encoders, it is advantageous to use the the IFSC scheme with the approach proposed in this chapter when the number of encoders (K) outnumber the number of transmitters (M), which translates to introducing a higher correlation between the observations of the encoders.

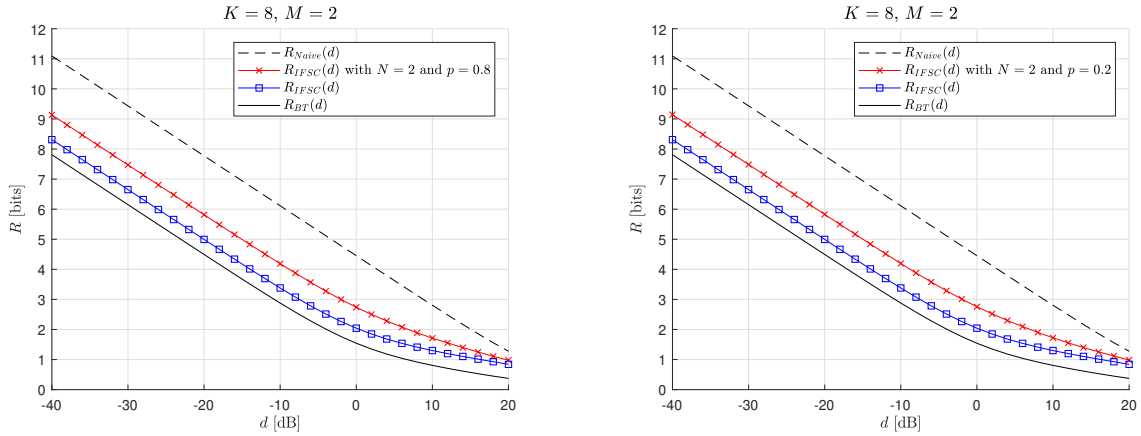


Figure 4.6: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.8$ and $p = 0.2$ in the setup $K = 8$ and $M = 2$. With $p = 0.8$ (a) and $p = 0.2$ (b) the rate-distortion curve is above the one considering a single covariance matrix for the IFSC scheme indicating a worse performance but is below the rate-distortion curve for the naive scheme, outperforming it. These two cases are symmetric.

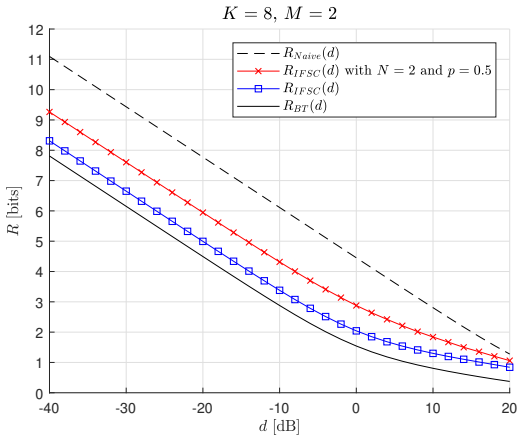
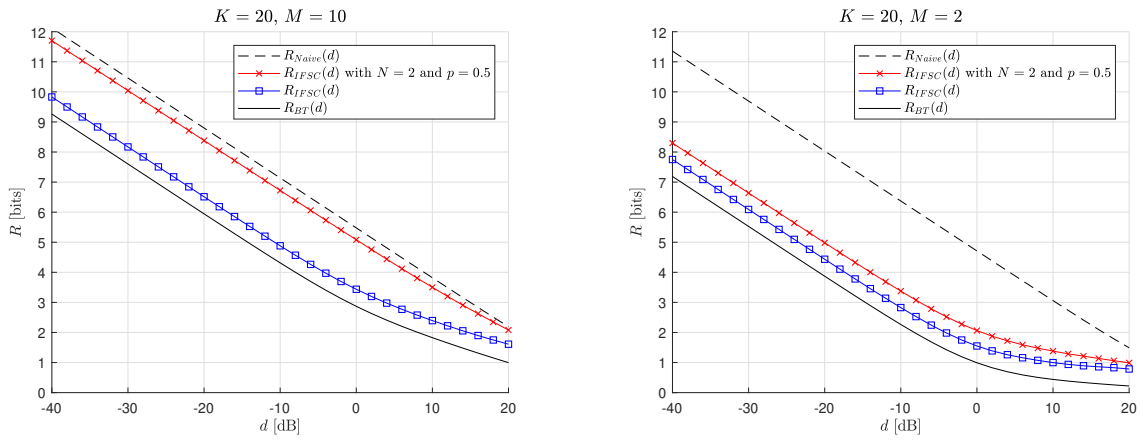


Figure 4.7: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.5$ in the setup $K = 8$ and $M = 2$. With $p = 0.5$ the rate-distortion curve is below the one considering a single covariance matrix for the naive scheme.

4.3.2 $N = 3$ Possible Covariance Matrices

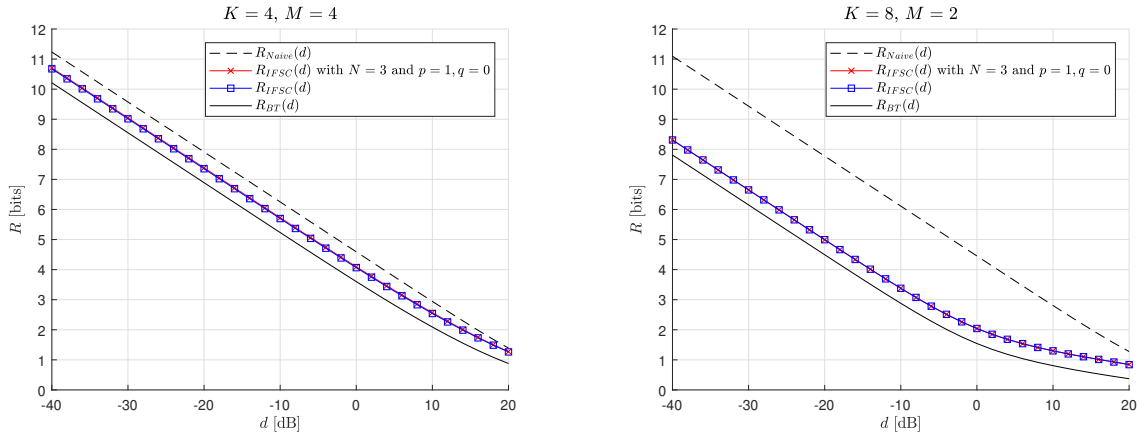
For a scenario with $N = 3$, three possible covariance matrices, $\mathbf{K_{xx}^A}$, $\mathbf{K_{xx}^B}$, and $\mathbf{K_{xx}^C}$, each having a probability $P(\mathbf{K_{xx}^A}) = p$, $P(\mathbf{K_{xx}^B}) = q$ and $P(\mathbf{K_{xx}^C}) = 1 - p - q$, respectively. For the considered setups with $K = M = 4$ and with $K = 8$ and $M = 2$, the rate-distortion curve obtained with $p = 1, q = 0$ matches the one obtained when considering the IFSC scheme with only one covariance matrix as depicted in figures 4.9(a) and 4.9(b). Due to the symmetry previously mentioned, the rate-distortion curves are equal for the cases with $p = 1, q = 0$, with $p = 0, q = 1$ and with $p = 0, q = 0$.

If one considers a covariance matrix with higher probability than the other covariance matrices in the set, the scheme is not adjusted to only one covariance matrix and creates a compromise as seen before. In figure 4.10 the simulations considering $p = 0.75, q = 0.125$ are presented for the setups $K = M = 4$ and $K = 8, M = 2$. Similarly to the binary case, even with the uncertainty regarding which of the three



(a) (b)

Figure 4.8: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.5$ in the setups $K = 20, M = 10$ and $K = 20, M = 2$. With the setup $K = 20, M = 10$ (a) the rate-distortion curve obtained with the IFSC scheme using the proposed approach is below the one obtained with the naive scheme but with the setup $K = 20, M = 2$ (b) the gap becomes larger.

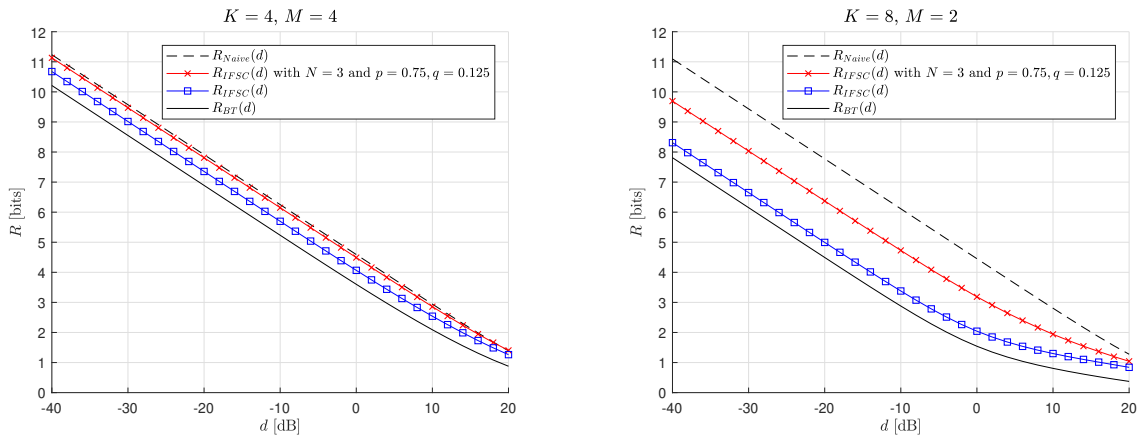


(a) (b)

Figure 4.9: Rate-distortion curves for $N = 3$ possible covariance matrices with $p = 1, q = 0$ for the setups $K = M = 4$ and $K = 8, M = 2$. For the setup with $K = M = 4$ (a) and the setup $K = 8, M = 2$ (b), the rate-distortion curve matches the one considering a single covariance matrix for the IFSC scheme.

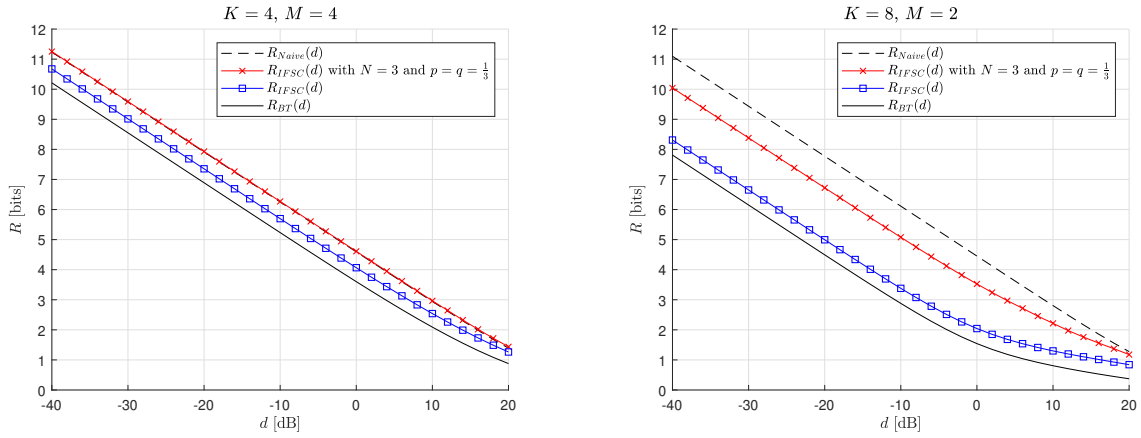
covariance matrices best describes the correlation between observations, the IFSC scheme with this proposed solution outperforms the naive scheme. Again, due to symmetry the rate-distortion curves are equal for the cases with $p = 0.75, q = 0.125$, with $p = 0.125, q = 0.75$ and with $p = 0.125, q = 0.125$.

For a situation with total uncertainty regarding which covariance matrix $\mathbf{K_{xx}^A}$, $\mathbf{K_{xx}^B}$ or $\mathbf{K_{xx}^C}$ is more appropriate to describe the existing correlations, i.e., when $p = q = \frac{1}{3}$, the same conclusions reached for the binary case can be drawn here. As observed in figure 4.11(a), the rate-distortion curve obtained matches the one obtained with the naive scheme, which means there is no difference in exploring the correlation between the observations of the encoders or not. However, in the case where there is a higher correlation between the observations as for the setup with $K = 8, M = 2$, the IFSC scheme using this approach outperforms the naive scheme as represented in figure 4.11(b).



(a) (b)

Figure 4.10: Rate-distortion curves for $N = 3$ possible covariance matrices with $p = 0.75, q = 0.125$ for the setups $K = M = 4$ and $K = 8, M = 2$. For the setup with $K = M = 4$ (a) and the setup $K = 8, M = 2$ (b), the rate-distortion curve is above the one considering a single covariance matrix for the IFSC scheme indicating a worse performance but is below the rate-distortion curve for the naive scheme, outperforming it.



(a) (b)

Figure 4.11: Rate-distortion curves for $N = 3$ possible covariance matrices with $p = q = \frac{1}{3}$ for the setups $K = M = 4$ and $K = 8, M = 2$. For the setup with $K = M = 4$ (a) the obtained rate-distortion curve matches the rate-distortion curve obtained with the naive scheme. For the setup with $K = 8, M = 2$ (b), the rate-distortion curve is below the rate-distortion curve obtained with the naive scheme.

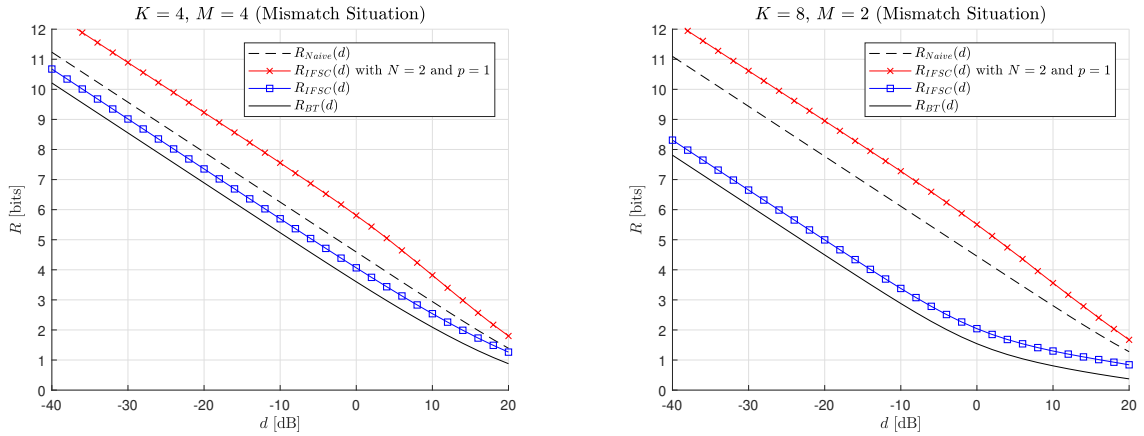
4.3.3 Mismatch of the Correlation Models

To further assess the proposed solution another simulation was made, this time with a mismatch between the probability of a given covariance matrix and its *true* probability of becoming the selected covariance matrix for which the rate rate $R_{IFSC}(d)$ is computed. This is of interest to infer what is the performance loss when this mismatch takes place and the scheme is not defined (with high probability) to deal with the correlation scenario. To exemplify this mismatch situation, the binary case is considered where two possible covariance matrices $\mathbf{K_{xx}^A}$ and $\mathbf{K_{xx}^B}$ have a probability $P(\mathbf{K_{xx}^A}) = p$ and $P(\mathbf{K_{xx}^B}) = 1 - p$. The

mismatch is created by considering that the selected covariance matrix is given by

$$\tilde{\mathbf{K}}_{\mathbf{xx}} = (1-\delta)\mathbf{K}_{\mathbf{xx}}^{\mathbf{A}} + \delta\mathbf{K}_{\mathbf{xx}}^{\mathbf{B}}. \tag{4.19}$$

instead of (4.5), where δ takes value 1 with probability p and value 0 with probability $1-p$. As a consequence of this mismatch, the IFSC scheme with the solution proposed in this chapter will compute, with the aid of the SM algorithm, an optimal matrix $\mathbf{A}_{\mathbf{ext}}^{*}$ that is more appropriate to a scenario with a lower probability. The compromise made is then unfair in the sense that it benefits a scenario that is not the most likely to occur. This causes a degradation in the performance of the IFSC scheme as observed by comparing figure 4.12(a) with figure 4.2(a) and figure 4.12(b) with figure 4.5(a) where $p = 1$ was set for both setups. These results are, as mentioned, equal to the ones obtained considering $p = 0$, and for this particular choice of values for p there is no advantage in terms of the attained performance in using the IFSC scheme instead of the naive approach.

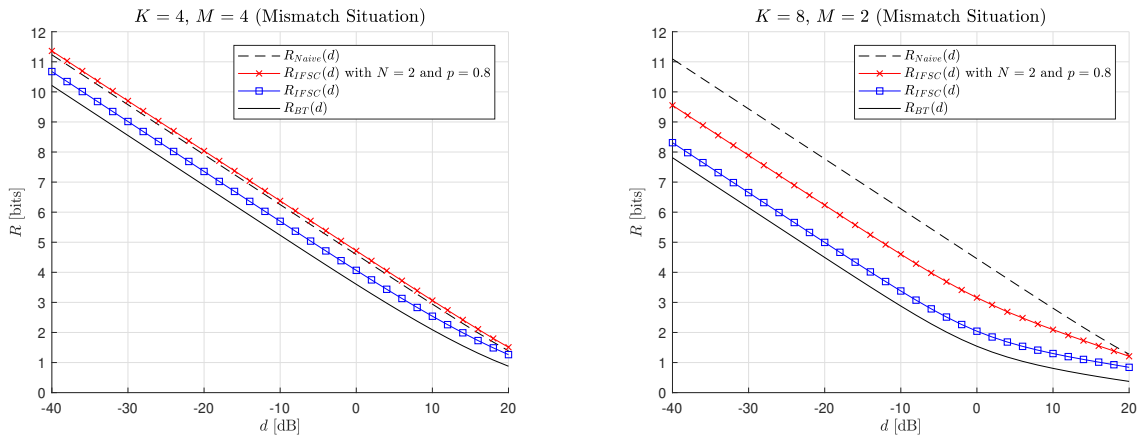


(a) (b)

Figure 4.12: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 1$ for the setups $K = M = 4$ (a) and $K = 8, M = 2$ (b) in a mismatch situation.

Furthermore, this performance degradation can be observed when setting $p = 0.8$ for both setups as represented in figures 4.13(a) and 4.13(b). For the setup with $K = 8, M = 2$ however, even with a performance degradation the IFSC scheme outperforms the naive coding scheme indicating that even with a mismatch situation it still is advantageous to exploit correlation. This can be further confirmed by extending the mismatch situation to the setup with $K = 20, M = 2$ as represented in figure 4.14.

To bring to a conclusion the discussion regarding this mismatch situation, the simulation results when considering $p = 0.5$ are presented in figure 4.15. As expected, these are equal to the results for the binary case with no mismatch situation since the covariance matrices are equally likely and the scheme does not benefit a particular one. With this in mind, figure 4.15(a) presents the same results as figure 4.4, and figure 4.15(b) the same results as figure 4.7.



(a) (b)

Figure 4.13: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.8$ for the setups $K = M = 4$ (a) and $K = 8, M = 2$ (b) in a mismatch situation.

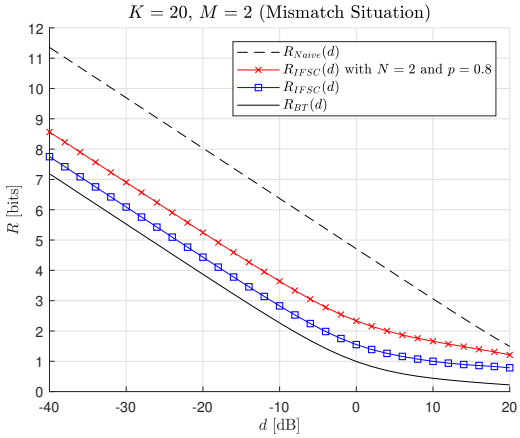
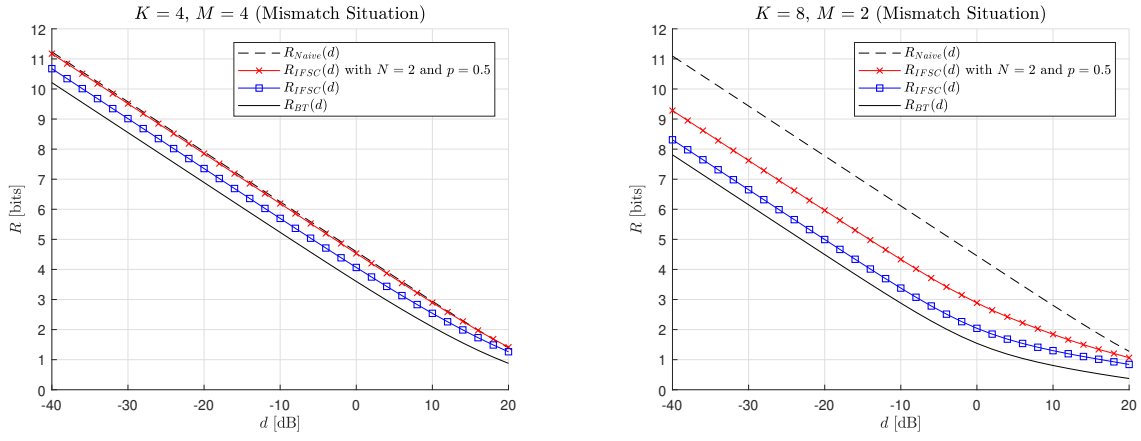


Figure 4.14: Rate-distortion curve for $N = 2$ possible covariance matrices with $p = 0.8$ for the setup with $K = 20, M = 2$ in a mismatch situation.



(a) (b)

Figure 4.15: Rate-distortion curves for $N = 2$ possible covariance matrices with $p = 0.5$ for the setups $K = M = 4$ (a) and $K = 8, M = 2$ (b) in a mismatch situation.

4.4 Closing Remarks

This chapter presents a solution to deal with the semi-blind correlation model where the IFSC scheme knows all the set of possible covariance matrices that can describe the correlation between the sources, but ignores which of these matrices best describes the correlation model for a given point in time. As mentioned, it is fundamental to this scheme to know in advance the set of possible covariance matrices and their respective probabilities in order to adapt its process to reach a compromise between them. This compromise is performed based on each individual probability so that the scheme is better suited to a covariance matrix with a higher probability than to the remaining ones.

An interesting feature of this proposed solution is that increasing the set size of possible correlations N does not increase the complexity of the underlying optimization problem to find $\mathbf{A}_{\mathbf{ext}}^{*}$. This is a consequence of the previously discussed "economy" QR decomposition and of lattice properties that allow the problem to be solved in a K-dimensional lattice, even if N is greater than K.

Further, as shown in the simulations of this proposed solution, even in the case of total uncertainty regarding which covariance matrix best describes the correlation model for a given point in time, i.e., the case where all the covariance matrices in the set are equally likely, it is advantageous in some cases to use the IFSC scheme rather than the naive scheme that does not exploit the correlation between sources. This is evident for the cases where there is enough correlation between sources as demonstraded in the previous sections.

Before ending this chapter it is also important to note that, even in a mismatch situation where the probability of a given covariance matrix does not match how appropriate the scheme is to it, the proposed solution outperforms the naive approach provided that there is enough correlation between the observations of the encoders.

Chapter 5

One-Shot Integer-Forcing Source Coding

In this chapter, the one-shot integer-forcing source coding (OIFSC) scheme is presented and compared to the original IFSC approach previously discussed in chapter 2.

5.1 Motivation for One-Shot Integer-Forcing

One of the main conclusions in [24] is that within the IFSC framework it is possible to trade-off complexity and performance. This trade-off is achieved by selecting which nested lattice codes are used in the IFSC scheme. By using high-dimensional pairs of nested lattices where the fine lattice used is good for MSE quantization and the coarse lattice is good for channel coding, the best performance is achieved (ideally, attaining the rate-distortions found in chapter 3). However, this leads to a complexity burden imposed on the encoders, which have to quantize their observations and perform modulo operations on these nested lattice pairs. For some applications, this complexity burden on the encoders side needs to be brought down to a minimum, and so, to tackle this problem a simpler version of the IFSC scheme is suggested in [24]. In this approach, the IFSC process is applied individually to each one of the n time realizations of the K observations retrieved by the K encoders. So, instead of using a n-D (n-dimensional) nested lattice pair, the OIFSC scheme requires only a 1-D nested lattice pair per dimension where both lattices are scaled versions of the integer lattice $\mathbb{Z}$. The reason for this decoupling of the dimensions comes from the orthogonality of both $\mathbb{Z}^n$ lattices.

In the following sections this low complexity scheme is defined, implemented, and simulated in order to measure the performance gap between the results obtained with 1-D nested lattice pairs and with high-dimensional nested lattice pairs with better geometric properties, considered in chapter 2. The performance of this simpler scheme is compared with the one attained with ideal non-orthogonal lattices when using the SM algorithm (described in chapter 3) that finds the optimal integer matrix $\mathbf{A}^*$.

5.2 1-D Nested Lattice Pair

Before defining the 1-D nested lattice pair used in the OIFSC scheme, it is important to revisit the definition of quantization noise. Given a quantization scheme like the one depicted in figure 5.1, with a quantization step size q that gives rise to a quantization error e, the probability density function of the quantization error is typically uniform over the quantization interval. Considering the rectangular function defined as

$$\text{rect}(x) = \begin{cases} 0 \text{ for } |x| > \frac{1}{2} \\ \frac{1}{2} \text{ for } |x| = \frac{1}{2} \\ 1 \text{ for } |x| < \frac{1}{2} \end{cases}, \tag{5.1}$$

the probability density function of the quantization error can be expressed by

$$\text{P}(e) = \frac{1}{q}\text{rect}\Big(\frac{e}{q}\Big), \tag{5.2}$$

as illustrated in figure 5.2.

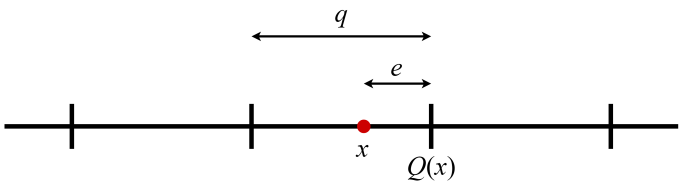


Figure 5.1: Quantization scheme with quantization step size q and quantization error e.

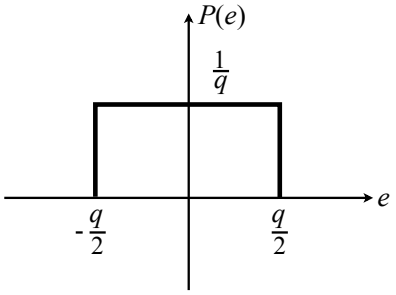


Figure 5.2: Probability density function of the quantization error e.

Let n_q^2 be the quantization noise power. Then,

$$n_q^2 \triangleq \mathbb{E}(e^2) = \int_{-\frac{q}{2}}^{\frac{q}{2}} e^2 \frac{1}{q}\, de = \frac{q^2}{12}, \tag{5.3}$$

and, denoting the MSE by d, which is equal to the quantization noise power n_q^2 in (5.3), one obtains the relation $q = \sqrt{12d}$.

After setting a quantization step q such that the OIFSC scheme achieves an average MSE d, it is possible to define a 1-D nested lattice pair such that the fine lattice is given by $\Lambda_f = \sqrt{12d}\,\mathbb{Z}$ and the coarse lattice by $\Lambda_c = 2^R\sqrt{12d}\,\mathbb{Z}$. As stated in [24], if 2^R is a positive integer then $\Lambda_c \subseteq \Lambda_f$ and the codebook $\mathcal{C} = \Lambda_f \cap \mathcal{V}_c$ has rate R, where $\mathcal{V}_c$ is the Voronoi region of the coarse lattice Λ_c, and it contains a valid codebook for IFSC. This nested lattice pair is represented in figure 5.3.

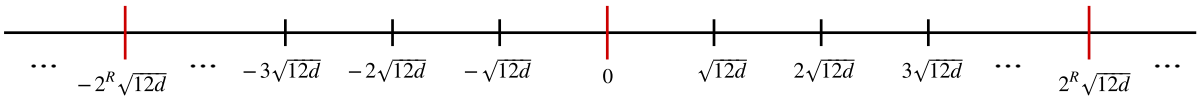


Figure 5.3: 1-D nested lattice pair used in the OIFSC scheme, where $\Lambda_c \subseteq \Lambda_f$. All the lattice points represented belong to the fine lattice Λ_f and only the points highlighted (longer red ticks) belong to the coarse lattice Λ_c.

5.3 One-Shot Integer-Forcing Source Coding Scheme

5.3.1 One-Shot Integer-Forcing Source Coding Scheme Definition

As was previously mentioned, in the OIFSC scheme, the IFSC process is applied individually to each one of the n time realizations of the K observations retrieved by the K encoders. One can refer to this as a per dimension slicing. If one considers a matrix $\mathbf{X}$ that represents the K observations over n time realizations of the form

$$\mathbf{X} \triangleq \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_K \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ & & \vdots & \\ x_{K1} & x_{K2} & \dots & x_{Kn} \end{bmatrix},$$

the per dimension slicing amounts to performing both the quantization to Λ_f and the modulo-Λ_c reduction to each element of each column of $\mathbf{X}$ independently of the other coordinates.

In order to have a quantization error uniformly distributed over the quantization interval, as it was specified in the previous section, a dithered quantization has to be applied as in the IFSC scheme of chapter 2. To apply this dithered quantization, a random dither vector $\mathbf{d}$, whose entries d_k are uniformly distributed over the Voronoi region of the fine lattice $\mathcal{V}_f$, is used. Every encoder in the OIFSC scheme has the same 1-D nested lattice pair defined in the previous section, and so, the kth encoder starts the process by adding the dither value d_k to its observation x_k and quantizing the result on the fine lattice Λ_f. It then proceeds by reducing this quantized point modulo-Λ_c, obtaining the lattice point

$$[Q_{\Lambda_f}(x_k + d_k)] \bmod \Lambda_c,$$

as depicted in figure 5.4. It is important to note that x_k represents the observation of the kth encoder at a given time realization n, where the index n is dropped.

At the decoder, the dither values are subtracted from the corresponding received points and the result is reduced modulo Λ_c to obtain

$$\begin{aligned}\tilde{x}_k &= \big[[Q_{\Lambda_f}(x_k + d_k)] \bmod \Lambda_c - d_k\big] \bmod \Lambda_c \\ &= \big[Q_{\Lambda_f}(x_k + d_k) - d_k\big] \bmod \Lambda_c \\ &= \big[x_k + Q_{\Lambda_f}(x_k + d_k) - (x_k + d_k)\big] \bmod \Lambda_c \\ &= \big[x_k + u_k\big] \bmod \Lambda_c,\end{aligned} \tag{5.4}$$

where the second transition follows from the distributive law (cf. appendix B) and u_k is the estimation error that is uniformly distributed over the quantization interval. With the optimal integer-valued full-rank matrix $\mathbf{A}^* \in \mathbb{Z}^{K\times K}$ obtained with the use of the LLL algorithm or the SM algorithm explored in the previous chapters, the decoder proceeds by computing linear combinations between the received $\tilde{x}_k$ for $k = 1, ..., K$. Afterwards, the decoder reduces those linear combinations modulo-Λ_c.

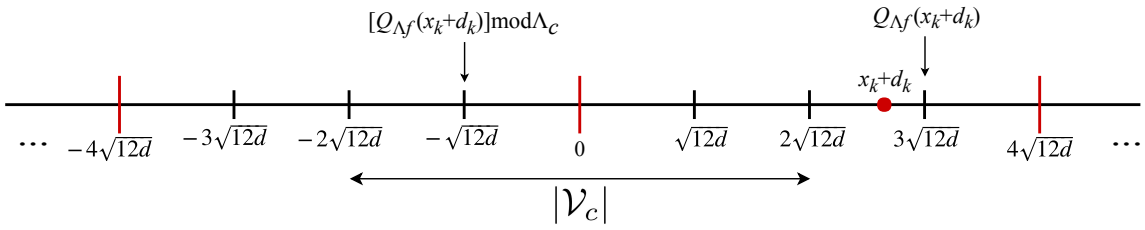


Figure 5.4: Example of the process performed by each one of the K encoders with a 1-D nested lattice pair having rate $R = 2$. The dimension of the Voronoi region of the coarse lattice, $|\mathcal{V}_c|$, is also represented.

This part of the process performed by the decoder can be summarized by

$$\begin{aligned}\widehat{\mathbf{Ax}} &\triangleq [\mathbf{A}\tilde{\mathbf{x}}] \bmod \Lambda_c \\ &= \big[\mathbf{A}[\mathbf{x} + \mathbf{u}] \bmod \Lambda_c\big] \bmod \Lambda_c \\ &= \big[\mathbf{A}(\mathbf{x} + \mathbf{u})\big] \bmod \Lambda_c,\end{aligned} \tag{5.5}$$

where $\mathbf{x}$ is one of the n columns of $\mathbf{X}$, $\mathbf{u}$ is the column vector containing the corresponding estimation errors, the modulo-Λ_c reduction is applied to each row, and the third step follows from the "general" distributive law for matrices (cf. appendix B). Finally, the decoder computes

$$\hat{\mathbf{x}} = \mathbf{A}^{-1}\widehat{\mathbf{Ax}}, \tag{5.6}$$

to obtain the estimate of $\mathbf{x}$. The block diagram of the OIFSC scheme is depicted in figure 5.5.

Similar to the case of IFSC with high-dimensional pairs of non-orthogonal nested lattices, the main feature of the OIFSC scheme is that it explores the correlation between the elements of $\mathbf{x}$ in such a way that the linear combinations between the elements of $\mathbf{x} + \mathbf{u}$ performed with the aid of an integer matrix $\mathbf{A}$ may have smaller variances than the original observations. Taking into account the 1-D nested lattice

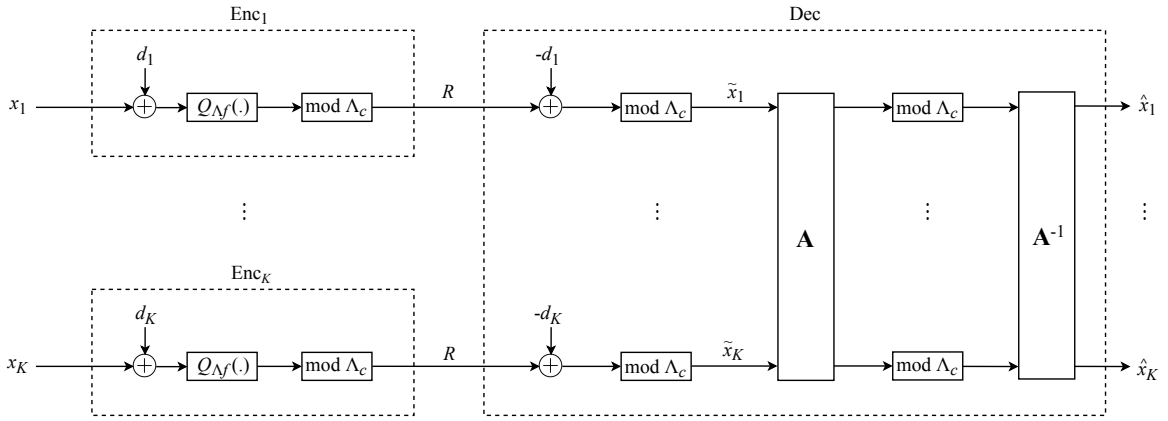


Figure 5.5: One-shot integer-forcing source coding scheme.

pair used, this scheme takes advantage of the fact that those linear combinations are more confined to the Voronoi region of Λ_c than the original observations, as presented in section 2.3.1. In other words, it explores the fact that

$$P(\mathbf{x} \notin \mathcal{V}_c) > P\big(\mathbf{A}(\mathbf{x}+\mathbf{u}) \notin \mathcal{V}_c\big), \tag{5.7}$$

and that $P\big(\mathbf{A}(\mathbf{x}+\mathbf{u}) \notin \mathcal{V}_c\big)$ is close to zero, meaning that the modulo-Λ_c reduction has no effect in (5.5), given that the points to be reduced modulo-Λ_c are already inside $\mathcal{V}_c$. In these conditions, the estimate of $\mathbf{x}$ is given by

$$\hat{\mathbf{x}} = \mathbf{A}^{-1}\mathbf{A}(\mathbf{x}+\mathbf{u}) = (\mathbf{x}+\mathbf{u}), \tag{5.8}$$

and the MSE attained by this scheme is

$$\mathbb{E}\big[(\mathbf{x}-\hat{\mathbf{x}})^2\big] = \mathbb{E}\big[(\mathbf{x}-(\mathbf{x}+\mathbf{u}))^2\big] = \mathbb{E}\big[\mathbf{u}^2\big] = d, \tag{5.9}$$

considering the estimation error $\mathbf{u}$ to be equal to the quantization error $\mathbf{e}$, and taking into account expression (5.3). At this point, it is important to note that the MSE attained by this scheme is different from the target distortion d. The "promise" of this scheme is that an MSE equal to d is attained when the integer linear combinations between $\mathbf{x}+\mathbf{u}$ are successfully enclosed in $\mathcal{V}_c$ so that (5.8) holds. If (5.8) does not hold, then the final MSE attained by the OIFSC scheme is higher than the target distortion d.

The probability that the linear combinations between the elements of $\mathbf{x}+\mathbf{u}$ are not confined to $\mathcal{V}_c$, $P\big(\mathbf{A}(\mathbf{x}+\mathbf{u}) \notin \mathcal{V}_c\big)$, can be made as low as desired when applying high-dimensional non-orthogonal nested lattice pairs. This is achieved by guaranteeing that $\mathcal{V}_c$ contains the "worst" linear combination, i.e., that $r_{eff}^2(\Lambda_c)$ is larger than the effective variance corresponding to that linear combination [24]. For the OIFSC scheme however, this probability is finite and its value depends on the linear size of the Voronoi region of the course lattice in each dimension: $2^R q = 2^R\sqrt{12d}$. The event where (5.8) does not hold can be referred to as the *overload* (OL) event that leads to an obtained MSE larger than d since there is loss of information when this event occurs. An upper bound for the probability of this event,

$P_{ol} \in [0,1]$, was given in [24] as

$$P_{ol} \leq 2K \exp\Big[-\frac{3}{2}2^{2[R-R_{IFSC}(d)]}\Big], \tag{5.10}$$

where $R_{IFSC}(d)$ is the rate attained with IFSC using a high-dimensional nested lattice pair of non-orthogonal lattices for a given target distortion d. This overload probability influences the rate penalty incurred when using the OIFSC scheme, i.e., in the difference $R - R_{IFSC}(d)$ that results from using a 1-D nested lattice pair. This rate penalty is derived from (5.10), coming as

$$\delta(P_{ol}) = \frac{1}{2}\log_2\Big(\frac{2}{3}\ln\frac{2K}{P_{ol}}\Big). \tag{5.11}$$

The question that arises at this point is the one of finding the required rate R and its corresponding probability P_{ol} such that the final MSE follows

$$\begin{aligned}\mathbb{E}\big[(x_k - \hat{x}_k)^2\big] &= \mathbb{E}\big[u_k^2\big] \\ &= \mathbb{E}\Big[u_k^2 \,|\, OL\Big]P_{ol} + \mathbb{E}\Big[u_k^2 \,|\, \overline{OL}\Big](1-P_{ol}) \\ &\leq d\end{aligned} \tag{5.12}$$

for $k = 1, ..., K$. $\mathbb{E}\Big[u_k^2 \,|\, OL\Big]$ is the MSE attained provided there was an overload event, and $\mathbb{E}\Big[u_k^2 \,|\, \overline{OL}\Big]$ is the MSE attained when no overload event takes place and (5.8) holds. An upper bound for the latter is given in [24] as

$$\begin{aligned}\mathbb{E}\Big[u_k^2 \,|\, \overline{OL}\Big] &= \frac{\mathbb{E}\big[u_k^2\big] - \mathbb{E}\Big[u_k^2 \,|\, OL\Big]P_{ol}}{1-P_{ol}} \\ &\leq \frac{d}{1-P_{ol}},\end{aligned} \tag{5.13}$$

but for the former no upper bound has been established in the literature. In order to find a closed expression from which the required rate R and the corresponding P_{ol} can be obtained such that (5.12) holds, first it is necessary to set this upper bound. This is made in the following section.

5.3.2 Upper Bound Definition

One starts by considering that

$$\mathbf{u} = \mathbf{A}^{-1}\widehat{\mathbf{A}\mathbf{x}} - \mathbf{x} \tag{5.14}$$

with

$$u_k = \mathbf{b}_k^T\,\widehat{\mathbf{A}\mathbf{x}} - x_k, \tag{5.15}$$

where $\widehat{\mathbf{A}\mathbf{x}}$ is given by expression (5.5) and $\mathbf{b}_k^T$ is the kth row of $\mathbf{A}^{-1}$. Additionally, one also considers that OL is a binary random variable that takes values 0 or 1, such that $\mathbb{E}\big[u_k^2 \,|\, OL\big] = \mathbb{E}\big[u_k^2 \,|\, OL = 1\big]$. Since u_k^2 is a function of x_k,

$$u_k^2(x_k) = (x_k - \hat{x}_k)^2, \tag{5.16}$$

from the definitions of expected value and conditional probability, one gets

$$\begin{aligned}\mathbb{E}\left[u_k^2(x_k)\,|\,OL=1\right] &= \int_{\mathbb{R}} u_k^2(x_k)P(x_k|OL=1)dx_k \\ &= \int_{\mathbb{R}} u_k^2(x_k)\frac{P(x_k,OL=1)}{P(OL=1)}dx_k.\end{aligned} \tag{5.17}$$

By restricting the integration domain to $\mathcal{D}_{OL=1}$, i.e., the domain of x_k where $OL=1$, one can write

$$\int_{\mathbb{R}} u_k^2(x_k)\frac{P(x_k,OL=1)}{P(OL=1)}dx_k = \int_{\mathcal{D}_{OL=1}} u_k^2(x_k)P(x_k)dx_k\frac{1}{P(OL=1)}. \tag{5.18}$$

To illustrate this step, an example is depicted in figure 5.6, where if one restricts x_k to domain $\mathcal{D}_{OL=1}$ then the joint probability $P(x_k,OL)$ is equal to $P(x_k)$.

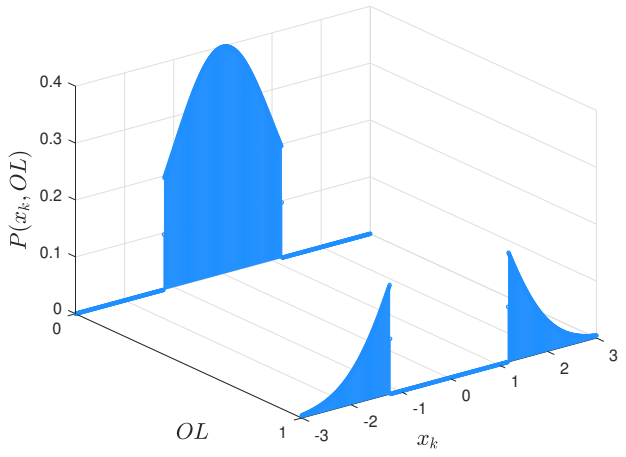


Figure 5.6: Joint probability $P(x_k,OL)$ in a 2-dimensional domain. By restricting x_k to domain $\mathcal{D}_{OL=1}$ or to domain $\mathcal{D}_{OL=0}$ the dependency on the random variable OL is lost and $P(x_k,OL)$ is equal to $P(x_k)$.

In order to upper bound $\mathbb{E}\left[u_k^2\,|\,OL\right]$, one has to upper bound the right side of expression (5.18). To do so, the strategy adopted was to first find an upper bound for

$$\int_{\mathcal{D}_{OL=1}} u_k^2(x_k)P(x_k)dx_k,$$

that shall be denoted Bound I, and then find an upper bound for

$$\frac{1}{P(OL=1)}$$

that shall be denoted Bound II. With this, the final upper bound is given by

$$\mathbb{E}\left[u_k^2\,|\,OL\right] \leq (\text{Bound I})(\text{Bound II}). \tag{5.19}$$

Bound I Definition

The first step is to note that

$$\begin{aligned}\int_{\mathcal{D}_{OL=1}} u_k^2(x_k)P(x_k)dx_k &\leq \int_{\mathbb{R}} u_k^2(x_k)P(x_k)dx_k \\ &= \mathbb{E}\big[u_k^2(x_k)\big].\end{aligned} \tag{5.20}$$

From expression (5.15), one has that

$$u_k^2(x_k) = (\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})^2 + x_k^2 - 2x_k(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}}), \tag{5.21}$$

and so

$$\begin{aligned}\mathbb{E}\big[u_k^2(x_k)\big] &= \mathbb{E}\Big[(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})^2 + x_k^2 - 2x_k(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})\Big] \\ &= \mathbb{E}\Big[\big(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}} + (-x_k)\big)^2\Big].\end{aligned} \tag{5.22}$$

Using the known inequality $(a+b)^2 \leq 2a^2 + 2b^2$, one can get

$$\big(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}} + (-x_k)\big)^2 \leq 2\big(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}}\big)^2 + 2x_k^2, \tag{5.23}$$

and one can upper bound (5.22) with

$$\mathbb{E}\Big[\big(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}} + (-x_k)\big)^2\Big] \leq \mathbb{E}\Big[2(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})^2 + 2x_k^2\Big]. \tag{5.24}$$

Using the theorem of appendix C and exploring the linearity of the expectation operator, one can further bound (5.24) to obtain

$$\begin{aligned}\mathbb{E}\Big[2(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})^2 + 2x_k^2\Big] &= 2\mathbb{E}\Big[(\mathbf{b}_k^T\,\widehat{\mathbf{Ax}})^2\Big] + 2\mathbb{E}\big[x_k^2\big] \\ &\leq 2\mathbb{E}\Big[\,\|\mathbf{b}_k\|_1^2\,\Big\|\widehat{\mathbf{Ax}}\Big\|_\infty^2\,\Big] + 2\mathbb{E}\big[x_k^2\big],\end{aligned} \tag{5.25}$$

where $\mathbf{b}_k$ is the transpose of the kth row of $\mathbf{A}^{-1}$. Expression (5.25) can be further upper bounded if one considers the highest value of $\mathbb{E}\big[x_k^2\big]$ for $k = 1, ..., K$ which is given by the maximum of the diagonal of the covariance matrix $\mathbf{K_{xx}}$,

$$\max_{k=1,\ldots,K} \mathbb{E}\big[x_k^2\big] = \max\big(\,\mathrm{diag}\,(\mathbf{K_{xx}})\big). \tag{5.26}$$

Moreover, if one considers the maximum value of $\|\mathbf{b}_k\|_1$ for $k = 1, ..., K$, that

$$\Big\|\widehat{\mathbf{Ax}}\Big\|_\infty \leq \frac{|\mathcal{V}_c|}{2}, \tag{5.27}$$

i.e., the integer linear combination with the highest absolute value among $\mathbf{A}(\mathbf{x}+\mathbf{u})$ reduced modulo-Λ_c

is always smaller than $\frac{|\mathcal{V}_c|}{2}$, and that by definition the size of the 1-D Voronoi region is $|\mathcal{V}_c| = 2^R q$, then:

$$\begin{aligned}\int_{\mathcal{D}_{OL=1}} u_k^2(x_k)P(x_k)dx_k \;&\leq\; 2\mathbb{E}\Big[\,\|\mathbf{b}_k\|_1^2\,\Big\|\widehat{\mathbf{Ax}}\Big\|_\infty^2\,\Big] + 2\max\big(\operatorname{diag}(\mathbf{K_{xx}})\big)\\ &= 2\,\|\mathbf{b}_k\|_1^2\,\Big\|\widehat{\mathbf{Ax}}\Big\|_\infty^2 + 2\max\big(\operatorname{diag}(\mathbf{K_{xx}})\big)\\ &\leq 2\max_{k=1,\ldots,K}\|\mathbf{b}_k\|_1^2\Big(\frac{2^R q}{2}\Big)^2 + 2\max\big(\operatorname{diag}(\mathbf{K_{xx}})\big).\end{aligned} \tag{5.28}$$

With this, the final expression for Bound I is given by

$$\text{Bound I} = 2\max_{k=1,\ldots,K}\|\mathbf{b}_k\|_1^2\Big(\frac{2^R q}{2}\Big)^2 + 2\max\big(\operatorname{diag}(\mathbf{K_{xx}})\big). \tag{5.29}$$

Bound II Definition

The strategy to find an expression to the other upper bound, Bound II, is to first lower bound $P(OL=1)$, which is defined as

$$P(OL=1) = P\big(\mathbf{A}(\mathbf{x}+\mathbf{u}) \notin \mathcal{V}_c\big). \tag{5.30}$$

Expanding (5.30), and using the union bound,

$$\begin{aligned}P(OL=1) &= P\big(\mathbf{A}(\mathbf{x}+\mathbf{u}) \notin \mathcal{V}_c\big)\\ &= P\Big(|\mathbf{a}_1^T(\mathbf{x}+\mathbf{u})| > \frac{2^R q}{2} \cup \ldots \cup |\mathbf{a}_K^T(\mathbf{x}+\mathbf{u})| > \frac{2^R q}{2}\Big)\\ &\geq \max_{k=1,\ldots,K} P\Big(|\mathbf{a}_k^T(\mathbf{x}+\mathbf{u})| > \frac{2^R q}{2}\Big),\end{aligned} \tag{5.31}$$

where, as mentioned before, $\mathbf{a}_k^T$ denotes the kth row of $\mathbf{A}$. The linear combination of Gaussian variables is also a Gaussian variable and therefore

$$\mathbf{a}_k^T(\mathbf{x}+\mathbf{u}) \sim \mathcal{N}\big(0, \mathbf{a}_k^T(\mathbf{K_{xx}} + d\mathbf{I})\mathbf{a}_k\big),$$

i.e., the integer linear combinations follow a Gaussian distribution with mean $\mu = 0$ and variance $\sigma^2 = \mathbf{a}_k^T(\mathbf{K_{xx}} + d\mathbf{I})\mathbf{a}_k$. The probability that such a Gaussian random variable with mean μ and variance σ^2 will have an observed value greater than $\mu + b\sigma$ is given by the Q-function

$$\mathrm{Q}(b) \triangleq \frac{1}{\sqrt{2\pi}}\int_b^\infty e^{-\frac{v^2}{2}}dv, \tag{5.32}$$

which accounts for the area under some defined tail of the Gaussian distribution [44]. Thus, defining

$$b = \frac{\frac{|\mathcal{V}_c|}{2} - \mu}{\sigma} = \frac{\frac{2^R q}{2} - \mu}{\sigma} = \frac{\frac{2^R q}{2}}{\sqrt{\mathbf{a}_k^T(\mathbf{K_{xx}} + d\mathbf{I})\mathbf{a}_k}}, \tag{5.33}$$

one has that

$$\begin{aligned} P\Big(|\mathbf{a}_k^T(\mathbf{x}+\mathbf{u})| > \frac{2^R q}{2}\Big) &= P\Big(\mathbf{a}_k^T(\mathbf{x}+\mathbf{u}) > \frac{2^R q}{2}\Big) + P\Big(\mathbf{a}_k^T(\mathbf{x}+\mathbf{u}) < -\frac{2^R q}{2}\Big) \\ &= 2P\Big(\mathbf{a}_k^T(\mathbf{x}+\mathbf{u}) > \frac{2^R q}{2}\Big) \\ &= 2\,\mathsf{Q}(b) \\ &= 2\,\mathsf{Q}\Big(\frac{2^R q}{2\sqrt{\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k}}\Big). \end{aligned} \tag{5.34}$$

Hence,

$$P(OL=1) \geq \max_{k=1,\ldots,K} 2\,\mathsf{Q}\Big(\frac{2^R q}{2\sqrt{\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k}}\Big), \tag{5.35}$$

and so Bound II is given by

$$\text{Bound II} = \frac{1}{\max_{k=1,\ldots,K} 2\,\mathsf{Q}\Big(\frac{2^R q}{2\sqrt{\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k}}\Big)}. \tag{5.36}$$

Final Upper Bound

With Bound I and Bound II defined, it is now possible to obtain an expression for the upper bound of $\mathbb{E}\Big[u_k^2 \,|\, OL\Big]$:

$$\begin{aligned} \mathbb{E}\Big[u_k^2 \,|\, OL\Big] &\leq (\text{Bound I})(\text{Bound II}) \\ &= \frac{\max_{k=1,\ldots,K} \|\mathbf{b}_k\|_1^2 \left(\frac{2^R q}{2}\right)^2 + \max\left(\operatorname{diag}\left(\mathbf{K_{xx}}\right)\right)}{\max_{k=1,\ldots,K} 2\,\mathsf{Q}\Big(\frac{2^R q}{2\sqrt{\mathbf{a}_k^T(\mathbf{K_{xx}}+d\mathbf{I})\mathbf{a}_k}}\Big)}. \end{aligned} \tag{5.37}$$

5.3.3 One-Shot Integer-Forcing Source Coding Scheme Implementation

With the OIFSC scheme defined and the previous upper bound established, it is now possible to design the implementation of this scheme such that the final MSE attained is smaller or equal than a given target distortion d as expressed by (5.12). As in the IFSC scheme, the encoders and the decoder have full knowledge about the correlation between the observations of the encoders expressed by $\mathbf{K_{xx}}$, and about the maximum target distortion d that the compression scheme is willing to accept. One can see $\mathbf{K_{xx}}$ and d as the input for the scheme's implementation from which the encoders and decoder have to agree on a number of parameters do design the pair of nested lattices.

One of these parameters is the optimal integer-valued full-rank matrix $\mathbf{A}^*$, the keystone of the OIFSC, which depends on it to perform integer linear combinations between the signals received by the decoder, as explained in the previous sections. This matrix is obtained by solving the aforementioned underlying optimization problem, that depends on $\mathbf{K_{xx}}$ and d, using either the SM algorithm or the LLL algorithm.

Another set of parameters that have to be defined is the rate R and the quantization step q such that (5.12) holds. To do so, one starts by considering a distortion value $\hat{d}$ that is smaller than the final target

distortion d, given by

$$\hat{d} = 0.99\, d, \tag{5.38}$$

and sets $\mathbb{E}\left[u_k^2 \,|\, \overline{OL}\right]$ to be equal to $\hat{d}$. With this distortion value, the quantization step q is computed by

$$q = \sqrt{12\hat{d}} \tag{5.39}$$

as defined in section 5.2. Next, one sets R to be equal to the rate attained by the IFSC scheme with high-dimensional non-orthogonal nested lattice pairs for the given target distortion d, $R_{IFSC}(d)$, obtained through expression (2.41). The corresponding P_{ol} is then calculated with (5.10), as well as the upper bound for $\mathbb{E}\left[u_k^2 \,|\, OL\right]$ with (5.37). If (5.12) does not hold with these values, R is increased by 0.01 bits, and one updates P_{ol} and the upper bound to revaluate if (5.12) holds. The update is repeated until a value for R is obtained such that (5.12) holds. This process is summarized in the form of pseudocode in Algorithm 4.

Algorithm 4 Algorithm to find R and q such that (5.12) holds.

Input: A target distortion d, a covariance matrix $\mathbf{K_{xx}}$, an optimal integer-valued full-rank matrix $\mathbf{A}^*$, and the rate attained by the original IFSC scheme for the given target distortion d, $R_{IFSC}(d)$.

Output: Rate R for the OIFSC scheme, quantization step q, and probability of an overload event P_{ol}.

1. Set $\hat{d} = 0.99\, d$ and $\mathbb{E}\left[u_k^2 \,|\, \overline{OL}\right] = \hat{d}$.
2. Initialize q with $q = \sqrt{12\hat{d}}$ and R with $R = R_{IFSC}(d)$.
3. Check if (5.12) holds. If it does, terminate and output R, q, and P_{ol}.
4. Increase R with 0.01 bits.
5. Update P_{ol} with (5.10) and the upper bound for $\mathbb{E}\left[u_k^2 \,|\, OL\right]$ with (5.37), and go to step 3.

With the rate R and the quantization step q defined, the 1-D nested lattice pair (Λ_f, Λ_c) can be constructed as presented in section 5.2. Furthermore, with a value for q the dither vector $\mathbf{d}$, used to guarantee that the estimation error is uniformly distributed over the quantizaton interval, can be obtained. Its entries are drawn from an uniform distribution on the interval $[-\frac{q}{2}, \frac{q}{2}]$, i.e., the Voronoi region of the 1-D fine lattice Λ_f. The 1-D nested lattice pair (Λ_f, Λ_c) and the dither vector $\mathbf{d}$ have to be available both at the encoders and at the decoder so that the OIFSC scheme works properly.

The just explained pre-processing required to implement the OIFSC scheme is summarized in the block diagram depicted in figure 5.7.

5.3.4 One-Shot Integer-Forcing Source Coding Scheme Performance

In order to assess the performance of the OIFSC scheme, an expression for the covariance matrix $\mathbf{K_{xx}}$ is required. For the sake of consistency in the performance comparison between the OIFSC scheme and the original IFSC scheme, the simulation example used in chapter 2 was also applied here. This example consists of a Gaussian network with M transmitting users and K non-cooperating encoders that try to compress a Gaussian source in a distributive manner $\mathbf{x} \in \mathbb{R}^{K\times 1}$ with zero mean and covariance matrix

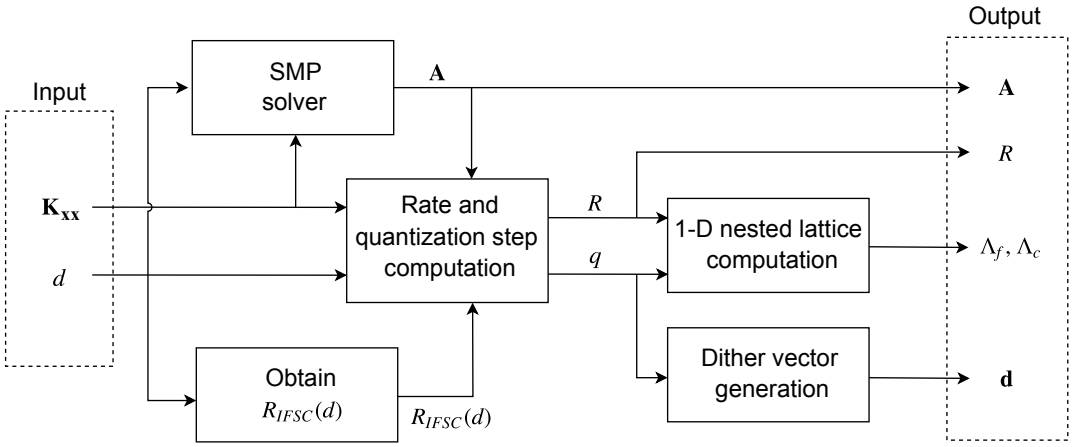


Figure 5.7: Block diagram of the pre-process required by the OIFSC scheme.

given by equation (2.1). As before, this Gaussian network serves the purpose of providing a correlation model for the observations of the encoders.

As in all other simulations in this work, the Berger-Tung benchmark provided in [24] is used as a lower bound. The other performance metric used throughout this thesis comes from the naive scheme. This scheme amounts to performing the IFSC scheme with high-dimensional nested lattice pairs without exploring the correlation between the observations of the encoders. Since one is interested in comparing the performance of the OIFSC scheme with its counterpart that does not explore the correlation across encoders, one has to compare the simulation results with the naive scheme metric plus the rate penalty required by the OIFSC scheme such that (5.12) holds, $R_{Naive}(d) + \delta(P_{ol})$. Besides these metrics, the rate-distortion curves corresponding to the IFSC scheme with high-dimensional non-orthogonal lattices with and without rate penalty, $R_{IFSC}(d) + \delta(P_{ol})$ and $R_{IFSC}(d)$, respectively. The SM algorithm presented in chapter 3 was used to solve the optimization problem that finds $\mathbf{A}^*$.

In the previous simulation results of this thesis, the rates presented for each target distortion d have been calculated for 1000 randomly generated covariance matrices $\mathbf{K_{xx}}$, and so, the final rate presented for that target distortion corresponded to the average of the rates computed over 1000 different correlation scenarios. Unlike these results, the simulation results of the OIFSC to be presented next were obtained considering only one covariance matrix $\mathbf{K_{xx}}$, randomly generated as before. Using this fixed covariance matrix, a source vector $\mathbf{x} \in \mathbb{R}^{K\times 1}$ was generated, and with it the OIFSC scheme was simulated as presented in the previous sections to obtain the MSE. This process of generating a source vector $\mathbf{x} \in \mathbb{R}^{K\times 1}$ was repeated 100 times for each target distortion in the interval of $[-40; 20]$ dB, always with the same covariance matrix $\mathbf{K_{xx}}$, in order to simulate the performance of this scheme over 100 time realizations with the same correlation model for the observations of the encoders. With this, the final MSE attained by the OIFSC scheme with rate R such that (5.12) holds for a given target distortion d, corresponds to the average of the MSE attained for each of those 100 time realizations. What is expected of the simulation results is that this final MSE is equal to the given target distortion d when considering a rate R. This attained rate-distortion curve is denoted as $R_{OIFSC}(d)$, and the algorithm

used to solve the underlying optimization problem was the SM algorithm presented in chapter 3.

The first setup considered was the one where $K = M = 4$. For this setup two different randomly generated covariance matrices were used to simulate the OIFSC scheme and to obtain the rate-distortion curves depicted in figures 5.8(a) and 5.8(b). In both these figures the rate penalty incurred by the use of a 1-D nested lattice pair instead of a high-dimensional nested lattice pair is about 2 bits, which is the required rate penalty in order to attain a final MSE equal to the specified target distortion d. This penalty rate of 2 bits allows, according to (5.10), a maximum probability of an overload event P_{ol} of about 3×10^{-10}, which is very low. As expected, the rate-distortion curve $R_{OIFSC}(d)$ is to the left of the rate-distortion curve $R_{IFSC}(d) + \delta(P_{ol})$ for both correlation scenarios, which indicates that the final MSE attained by the OIFSC scheme is in fact smaller than each target distortion.

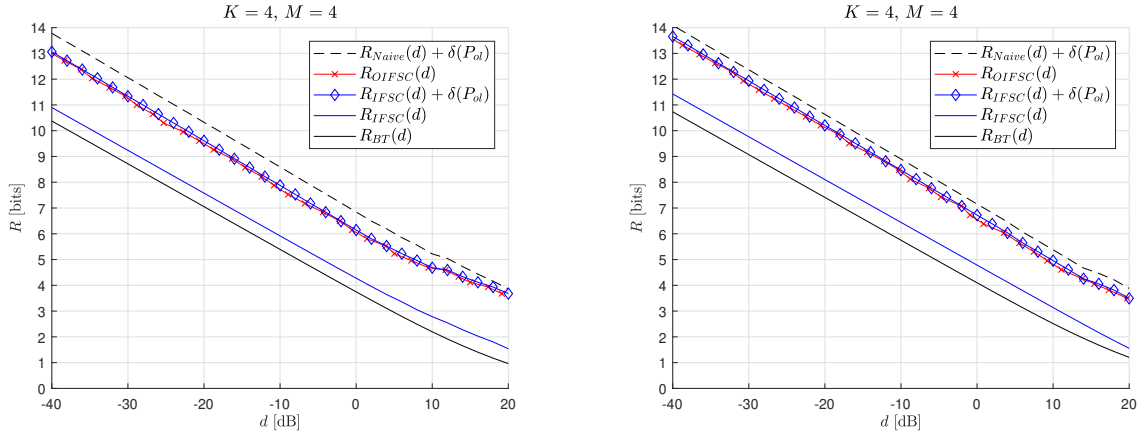


Figure 5.8: One-shot integer-forcing source coding rate-distortion curves for the setup with $K = M = 4$. Two different randomly generated covariance matrices were considered to obtain the rate-distortion curves in (a) and in (b).

Next, the setup with $K = 8$ and $M = 2$ was considered to simulate the OIFSC scheme. The obtained rate-distortion curves for two different covariance matrices are depicted in figures 5.9(a) and 5.9(b). As it is possible to observe, the same penalty rate of about 2 bits is required to guarantee that the final MSE is smaller or equal than each target distortion d. With this penalty rate, the maximum P_{ol} doubles with respect to the previous setup to 6×10^{-10} but remains a low value.

To further assess the implementation proposed in this chapter for the OIFSC scheme, two setups with $K = 20$ were simulated. The rate-distortion curves for the setup with $K = M = 20$, and for the setup with $K = 20$ and $M = 2$ are represented in figures 5.10(a) and 5.10(b), respectively. As observed in these figures, the required penalty rate is, once again, of about 2 bits in order to attain a final MSE smaller or equal than each target distortion d. With this penalty rate and $K = 20$, the maximum P_{ol} according to (5.10) is approximately 1.5×10^{-9}, which is still negligible.

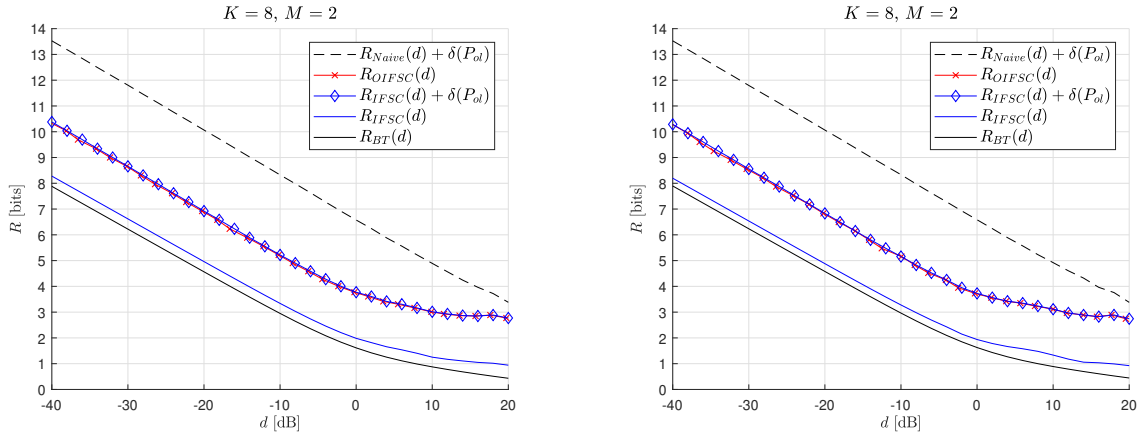


Figure 5.9: One-shot integer-forcing source coding rate-distortion curves for the setup with $K = 8$, $M = 2$. Two different randomly generated covariance matrices were considered to obtain the rate-distortion curves in (a) and in (b).

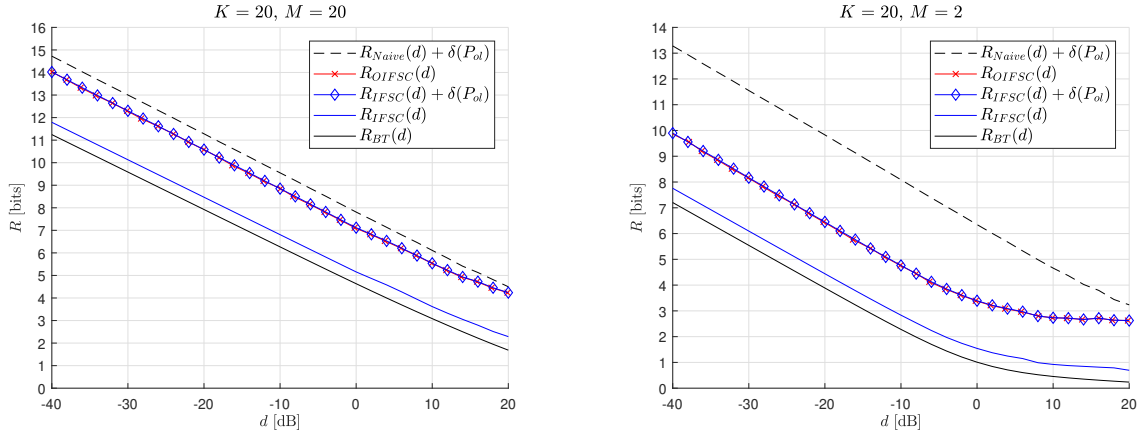


Figure 5.10: One-shot integer-forcing source coding rate-distortion curves for the setups with $K = M = 20$ (a) and with $K = 20$, $M = 2$ (b).

5.4 Closing Remarks

In this chapter a simpler version of the original IFSC scheme initially presented in chapter 2 was defined. This OIFSC scheme allows a lower complexity burden on the encoders and decoder of the lossy distributed source coding scheme since it relies on an 1-dimensional nested lattice pair instead of a high-dimensional nested lattice pair. One should however note that this is an instance of the theory laid in chapter 2 for constructions based on nested lattices, only that in this case both lattices are orthogonal and the processing in each dimension can be decoupled from the others.

This low-complexity architecture implies a performance degradation, as was shown in the previous section. This performance degradation translates to the need of having a higher required rate, when compared to the original IFSC scheme, to attain a final MSE smaller or equal to a specified target

distortion d.

In order to find the necessary rate increase, this chapter proposed a pre-processing for the OIFSC scheme, where the rate is found according to an upper bound, also provided in this chapter. This upper bound is formulated with the purpose of controlling the final MSE attained by the scheme so that it does not exceed the predefined maximum distortion allowed for the lossy distributed compression scheme. By means of simulation, this required rate was found to be roughly 2 bits per sample per encoder above the required rate for the original IFSC scheme at any distortion value in all the setups considered. These 2 extra bits lead, for example, for the setup with $K = 20$, to a probability of an overload event, i.e., the event where the decoder can not recover the original sources with a maximum distortion d, of approximately 1.5×10^{-9}, which can be neglected.

Chapter 6

Conclusions

In this final chapter, an overview of the main conclusions drawn throghout this thesis are presented. In addition, some suggestions for possible future work will be proposed.

6.1 Overall Conclusions

The contributions of this work lie in the framework of DSC, which encompasses a wide range of applications where it is beneficial to exploit the existing correlation between the information sources in order to code them in a more efficient manner. By exploiting that correlation, it is possible to reduce the power consumption of the encoding devices. In the scenarios considered in this work, the encoders are not able to exchange information among them and, at the same time, it is assumed that the decoder has enough computational power to perform joint decoding of the signals it receives from each encoder. The thesis focused on a recently proposed IFSC scheme that, while requiring some sizable complexity at the encoders in order to attain the information-theoretic limits, also has low-complexity and practical implementation that, for some configurations, still provides a huge performance gain in terms of the achieved rate-distortion curves.

The IFSC scheme presented and analyzed in this work exploits this correlation by means of integer linear combinations between the incoming signals at the decoder's side. By doing so, the required rate for the encoders to compress their observations within a maximum distortion value can be significantly reduced, as concluded in chapter 2. Paramount to IFSC is the requirement that both the encoders and the decoder use the same nested lattice codebook of dimension n, the number of time realizations of the source retrieved by each encoder. As stated, the final MSE per dimension attained by this scheme approaches the maximum target distortion when n approaches infinity. This may be inconvenient in the sense that the encoders have to quantize their observations in a n-dimensional nested lattice pair, which is not a low complexity operation.

One of the contributions of this thesis is a clarification of the underlying geometry of the concept of dealing with integer linear combinations of lattice-quantized sources, thus making evident why that allows a rate reduction. Until now this had remained rather unclear in the literature.

The integer linear combinations operation of IFSC induces the optimization problem of finding the optimal integer coefficients that span the shortest independent points of a K-dimensional lattice, K being the number of encoders in the scheme. As a first approach, this problem is solved using a LLL lattice reduction algorithm that yields a solution which is a good approximation for small values of K. For increasing K, however, this solution becomes a poor approximation, as the LLL algorithm fails to find the shortest basis of a lattice. To address this situation, an alternative algorithm very recently proposed in the literature was presented in chapter 3. This algorithm yields the exact solution (i.e., finds the K successive minima of a lattice), at the cost of increasing the time complexity from $\mathcal{O}(K^4 \log K)$ to $\mathcal{O}\big(K^{\frac{5}{2}}(2\pi e)^{\frac{K}{2}}\big)$, i.e., from polynomial to exponential running time. With this exact algorithm, the information-theoretic rate-distortion attained by the IFSC scheme was provided for some values of K up to $K = 25$.

Chapter 4 deals with the problem of having uncertainty about the model that describes the correlation between the sources. To tackle that problem, a new technique for IFSC was devised that takes in consideration the probabilities of each one of the possible correlation models, outputting integer matrices that are more oriented towards the correlation model with higher probability. Intuitively, this uncertainty leads to a performance degradation with respect to the rate-distortion attained with the IFSC scheme when considering only a fixed correlation model, as observed in the simulation results provided. However, even in the case of total uncertainty regarding the correlation model that best describes the existing correlation, it was seen by simulations that it is advantageous to use the IFSC scheme with the proposed solution, rather than a naive scheme that does not exploit this correlation. Furthermore, it was seen that even in a mismatch situation, where the true probability of a given correlation model does not match what was expected *a priori*, the IFSC scheme with the proposed solution outperforms the scheme with no correlation exploitation, provided that there exists enough correlation between the sources to be compressed. An interesting and relevant feature of this proposed solution, is that the underlying optimization problem does not increase in complexity when the set of possible correlation scenarios increases, depending only on the number of encoders in the system.

Finally, to approach the limitation imposed on the encoders by the use of high-dimensional nested lattice pairs, the one-shot version of IFSC was defined and analyzed. Also, a suggestion for the pre-process of this scheme was made with the purpose of controlling the performance degradation imposed by the use of an 1-dimensional nested lattice pair. By analyzing the simulation results of this low-complexity scheme, it was possible to conclude that the suggested pre-process works and the scheme attains a final MSE smaller to or equal than the given target distortion. Furthermore, a rate penalty of 2 bits was found to be sufficient for all the setups considered, leading to probabilities of overload than can be neglected.

6.2 Future Work

The work presented in this thesis opens the possibility to at least two possible research paths:

Erasure channel - In the model considered in this work, no errors or erasures are assumed between

the relays and the final destination. A first extension to this work would be to consider that some of the symbols cannot be read by the destination, declaring an erasure. One simple approach to deal with this missing data would be to take advantage of the spatial correlation between the samples, i.e., the correlation between the samples in each column of $\mathbf{X}$. One could solve the problem for the received dimensions (running a lower-dimensional IFSC optimization problem), retrieving the components for which the observations were received, and then using basic inference to assume that the missing component is given by the expected value of the missing random variable conditioned on the remaining estimated ones.

Temporal correlation - The model used in this thesis (which is also the one used in [24]) only assumes a spatial correlation between the samples, i.e., the samples taken within the same time-slot. In many applications one should expect to also find that the samples of the same source should hold some correlation along time. That is, the matrix $\mathbf{X}$ displays correlation in both its columns and its rows. The question is how to incorporate this new entanglement in an IFSC scheme. A first (simple) approach to this problem could be running in parallel two IFSC schemes, one for $\mathbf{X}$ and another one for $\mathbf{X}^T$, that is, considering the time correlation as playing the role of the spatial correlation (as in the scheme considered in this work). This can be seen as running IFSC for $\mathbf{AX}$ (as done throughout this dissertation) or, running IFSC for $\mathbf{XB}$, with $\mathbf{B}$ being an integer-valued full-rank matrix that linearly combines the columns of $\mathbf{X}$. In the end, one would opt for the case attaining the best information-theoretic performance (which depends on the $\mathbf{A}^*$ and $\mathbf{B}^*$ matrices found).

Bibliography

[1] C. E. Shannon. “A mathematical theory of communication”. *Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948.

[2] M. Effros and H. V. Poor. “Claude Shannon: His Work and Its Legacy”. *Newsletter of the European Mathematical Society Newsletter*, pp. 29-34, Mar. 2017.

[3] C. E. Shannon. “Coding theorems for a discrete source with a fidelity criterion”. *IRE International Convention Record*, vol. 7, pp. 142-163, 1959.

[4] D. Slepian and J. K. Wolf. “Noiseless coding of correlated information sources”. *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471-480, July 1973.

[5] A. D. Wyner and J. Ziv. “The rate-distortion function for source coding with side information at the decoder”. *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1-10, Jan. 1976.

[6] T. M. Cover. “A proof of the data compression theorem of Slepian and Wolf for ergodic sources (corresp.)”. *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 226-228, Mar. 1975.

[7] T. M. Cover, A. E. Gamal, and M. Salehi. “Multiple access channels with arbitrarily correlated sources”. *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 648-657, Nov. 1980.

[8] R. Cristescu, B. Beferull-Lozano, and M. Vetterli. “Networked Slepian-Wolf: theory, algorithms, and scaling laws”. *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4057-4073, Dec. 2005.

[9] J. Barros and S. D. Servetto. “Network information flow with correlated sources”. *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 155-170, Jan. 2006.

[10] P.-S. Lu, X. Zhou, and T. Matsumoto. “Outage probabilities of orthogonal multiple-access relaying techniques with imperfect source-relay links”. *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 2269-2280, Apr. 2015.

[11] A. J. Aljohani, S. X. Ng, and L. Hanzo. “Distributed Source Coding and Its Applications in Relaying-Based Transmission”. *IEEE Access*, vol. 4, pp.1940-1970, Mar. 2016.

[12] T. Berger. “Multiterminal source coding”. In *Proc. Lectures Presented CISM Summer School Information Theory Approach Community*, pages 171–231, July 1977.

[13] C. Heegard and T. Berger. “Rate distortion when side information may be absent”. *IEEE Transactions on Information Theory*, vol. 31, no. 6, pp. 727-734, Nov. 1985.

[14] R. Zamir. “The rate loss in the wyner-ziv problem”. *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2073-2084, Nov. 1996.

[15] Y. Oohama. “Gaussian multiterminal source coding”. *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1912-1923, Nov. 1997.

[16] R. Zamir, S. Shamai, and U. Erez. “Nested Linear/Lattice Codes for Structured Multiterminal Binning”. *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1250-1276, June 2002.

[17] Y. Yang, V. Stankovic, Z. Xiong, and W. Zhao. “On multiterminal source code design”. *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2278-2302, Apr. 2008.

[18] Y. Oohama. “Indirect and direct gaussian distributed source coding problems”. *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7506-7539, Oct. 2014.

[19] J. Garcia-Frias and Z. Xiong. “Distributed source coding and joint source-channel coding: From theory to practice”. In *Proc. IEEE International Conference Acoustics, Speech, and Signal Processing (ICASSP)*, volume 5, pages 1093–1096, Philadelphia, PA, USA, Mar. 2005.

[20] Z. Xiong, A. Liveris, and S. Cheng. “Distributed Source Coding for Sensor Networks”. *IEEE Signal Processing Magazine*, vol. 21, no. 5, pp. 80-94, Sept. 2004.

[21] J. Zhan, B. Nazer, U. Erez, and M. Gastpar. “Integer-Forcing Linear Receivers”. *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7661-7685, Dec. 2014.

[22] L. Zheng and D. N. C. Tse. “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels”. *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.

[23] O. Ordentlich and U. Erez. “Precoded integer-forcing universally achieves the mimo capacity to within a constant gap”. *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 323-340, Jan. 2015.

[24] O. Ordentlich and U. Erez. “Integer-Forcing Source Coding”. *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1253-1269, Feb. 2017.

[25] E. Domanovitz and U. Erez. “Outage probability bounds for integer-forcing source coding”. In *IEEE Information Theory Workshop (ITW)*, pages 574–578, Kaohsiung, Taiwan, Nov. 2017.

[26] A. K. Lenstra, H. W. Lenstra, and L. Lovász. “Factoring polynomials with rational coefficients”. *Mathematische Annalen*, vol. 261, no. 4, pp. 515-534, 1982.

[27] F. A. Monteiro, I. J. Wassell, and N. Souto. *MIMO Detection Methods*, chapter 2, pages 47–117. CRC Press / Taylor & Francis Group, FL, USA, 2014.

[28] C. Feng, D. Silva, and F. Kschischang. ”An Algebraic Approach to Physical-Layer Network Coding”. In *2010 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 1017–1021, June 2010.

[29] B. Nazer and M. Gastpar. ”Reliable Physical Layer Network Coding”. *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438 - 460, Mar. 2011.

[30] P. L. Dragotti and M. Gastpar. *Distributed Source Coding: Theory, Algorithms and Applications*. Academic Press, 2009.

[31] R. Zamir. *Lattice Coding for Signals and Networks*. Cambridge, U.K.: Cambridge University Press, 2014.

[32] A. Banihashemi. *“Decoding Complexity and Trellis Structure of Lattices”*. PhD thesis, University of Waterloo, 1997.

[33] J. Wen, L. Li, X. Tang, W. H. Mow, and C. Tellambura. “An Exact Algorithm for the Optimal Integer Coefficient Matrix in Integer-Forcing Linear MIMO Receivers”. presented at the 2017 IEEE International Conference on Communications (ICC), Feb. 2017.

[34] ”Dither”. Web platform: *https://en.wikipedia.org/wiki/Dither* [May 2018].

[35] U. Erez and R. Zamir. “Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding”. *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293-2314, Oct. 2004.

[36] O. Ordentlich and U. Erez. “A Simple Proof for the Existance of “Good” Pairs of Nested Lattices”. *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4439-4453, Aug. 2016.

[37] S.-Y. Tung. *“Multiterminal source coding”*. PhD thesis, School of Electrical Engineering, Cornell University, Ithaca, NY, USA, 1978.

[38] S. Wang, Y. Fang, and S. Cheng. *Distributed Source Coding: Theory and Practice*. Wiley, 2017.

[39] L. Ding, K. Kansanen, and Y. Wang. “Exact SMP algorithms for integer-forcing linear MIMO receivers”. *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6955-6966, Dec. 2015.

[40] J. Wen and X.-W. Chang. “A KZ Reduction Algorithm”. submitted to IEEE Transactions on Wireless Communications, 2017.

[41] C.-P. Schnorr. “A hierarchy of polynomial time lattice basis reduction algorithms”. *IEEE Transactions on Communications*, vol. 53, pp. 201-224, 1987.

[42] S. Epp. *Discrete Mathematics with Applications*, chapter 11, pages 725–729. Richard Stratton, 4th edition, 2011.

[43] C. Ling, W. H. Mow, and N. Howgrave-Graham. “Reduced and Fixed-Complexity Variants of the LLL Algorithm for Communications”. *IEEE Transactions on Communications*, vol. 61, no. 3, pp. 1040-1050, Mar. 2013.

[44] P. B. Crilly and A. B. Carlson. *Communication Systems*, pages 857–858. McGraw-Hill Education, 5th edition, 2009.

Appendix A

Lattice “goodness” properties

This appendix provides useful definitions regarding lattice “goodness” properties that are of use to the theoretic foundations of IFSC, as laid out in [24].

Definition A.1 (Goodness for MSE quantization)**.** A n-dimensional lattice Λ is said to be good for MSE quantization if

$$\lim_{n\to\infty} \sigma^2(\Lambda) = \lim_{n\to\infty} \frac{r_{eff}^2(\Lambda)}{n}. \tag{A.1}$$

Definition A.2 (Semi norm-ergodic noise)**.** A random noise vector $\mathbf{z}$ with finite effective variance given by

$$\sigma_{\mathbf{z}}^2 = \frac{\mathbb{E}(\|\mathbf{z}\|^2)}{n}, \tag{A.2}$$

is semi norm-ergodic if for any $\varepsilon > 0$, $\delta > 0$ and n large enough

$$P\big(\,\|\mathbf{z}\| > \sqrt{(1+\delta)n\sigma_{\mathbf{z}}^2}\big) \leq \varepsilon. \tag{A.3}$$

Lemma. Let $\mathbf{u}_1, ..., \mathbf{u}_K$ be statistically independent random vectors, each uniformly distributed over the Voronoi region $\mathcal{V}$ of a lattice Λ that is good for MSE quantization. Let $\mathbf{z}$ be an i.i.d. random vector statistically independent of $\mathbf{u}_1, ..., \mathbf{u}_K$. For any α and $\beta_1, ..., \beta_K \in \mathbb{R}$ the random vector given by

$$\alpha\mathbf{z} + \sum_{k=1}^{K} \beta_k \mathbf{u}_k$$

is semi norm-ergodic.

Definition A.3 (Goodness for channel coding)**.** A n-dimensional lattice Λ is said to be good for channel coding if for any $0 < \delta < 1$ and any n-dimensional semi norm-ergodic vector $\mathbf{z}$ with zero mean and effective variance given by

$$\frac{\mathbb{E}(\|\mathbf{z}\|^2)}{n} < (1-\delta)\frac{r_{eff}^2(\Lambda)}{n}, \tag{A.4}$$

one has that

$$\lim_{n\to\infty} P(\mathbf{z} \notin \mathcal{V}) = 0. \tag{A.5}$$

Appendix B

Modulo-lattice properties

In this appendix the modulo-lattice properties are stated and the respective proofs are provided. The proof of the modulo-Λ invariance under lattice point shifting is a basic concept of lattice theory and can easily found in the literature (e.g., [31]). However, the general distributive law for matrices, that is central in IFSC [24], is usually used without a rigorous proof being given, and for that reason the property is here derived.

Definition B.1 (Modulo-Λ reduction)**.** For a given lattice Λ, the modulo-Λ reduction is defined as

$$[\mathbf{x}] \bmod \Lambda = \mathbf{e} = \mathbf{x} - Q_\Lambda(\mathbf{x}) \tag{B.1}$$

where **e** is the quantization error, and $Q_\Lambda(\mathbf{x})$ is a lattice point and denotes the quantization of $\mathbf{x}$ into Λ.

Theorem B.1 (Modulo-Λ invariance under lattice point shifting)**.** For any lattice point $\lambda \in \Lambda$ and a vector $\mathbf{x} \in \mathbb{R}^n$ one has that

$$\begin{aligned} [\mathbf{x} + \lambda] \bmod \Lambda &= [\mathbf{x}] \bmod \Lambda \\ (\mathbf{x} + \lambda)_r &= \mathbf{x}_r, \end{aligned} \tag{B.2}$$

where the index "r" stands for "reduced (modulo-Λ)" .

Proof. This results from the modulo-Λ reduction definition, where adding any lattice point λ to $\mathbf{x}$ and then reducing the result modulo-Λ has no effect in the end. □

Theorem B.2 (Distributive law)**.** For two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ one has that

$$\begin{aligned} \big[[\mathbf{x}] \bmod \Lambda + \mathbf{y}\big] \bmod \Lambda &= [\mathbf{x} + \mathbf{y}] \bmod \Lambda \\ (\mathbf{x}_r + \mathbf{y})_r &= (\mathbf{x} + \mathbf{y})_r. \end{aligned} \tag{B.3}$$

Proof. The inner modulo operation amounts to shifting $\mathbf{x}$ by $Q_\Lambda(\mathbf{x}) \in \Lambda$ and, using theorem B.1,

$$\begin{aligned} \big[[\mathbf{x}] \bmod \Lambda + \mathbf{y}\big] \bmod \Lambda &= [\mathbf{x} - Q_\Lambda(\mathbf{x}) + \mathbf{y}] \bmod \Lambda \\ &= [\mathbf{x} + \mathbf{y}] \bmod \Lambda. \end{aligned} \tag{B.4}$$

□

Theorem B.3 ("Restricted" distributive law)**.** For two vectors $\mathbf{x}$, $\mathbf{y} \in \mathbb{R}^n$ and $a \in \mathbb{Z}$ one has that

$$\begin{aligned} [a[\mathbf{x}] \bmod \Lambda + \mathbf{y}] \bmod \Lambda &= [a\mathbf{x} + \mathbf{y}] \bmod \Lambda \\ (a\mathbf{x}_r + \mathbf{y})_r &= (a\mathbf{x} + \mathbf{y})_r. \end{aligned} \tag{B.5}$$

Proof. By applying theorem B.1 again one obtains

$$\begin{aligned} [a[\mathbf{x}] \bmod \Lambda + \mathbf{y}] \bmod \Lambda &= [a(\mathbf{x} - Q_\Lambda(\mathbf{x})) + \mathbf{y}] \bmod \Lambda \\ &= [a\mathbf{x} - aQ_\Lambda(\mathbf{x}) + \mathbf{y}] \bmod \Lambda \\ &= [a\mathbf{x} + \mathbf{y} - aQ_\Lambda(\mathbf{x})] \bmod \Lambda \\ &= [a\mathbf{x} + \mathbf{y}] \bmod \Lambda, \end{aligned} \tag{B.6}$$

since $aQ_\Lambda(\mathbf{x})$ is a lattice point according to lattice properties. □

Theorem B.4 ("General" distributive law)**.** For a set of vectors $\mathbf{x}_i \in \mathbb{R}^n$ for $i = 1, ..., K$, a vector $\mathbf{y} \in \mathbb{R}^n$ and a set of integers $a_i \in \mathbb{Z}$ for $i = 1, ..., K$ one has that

$$\begin{aligned} \Big[\sum_i^K a_i[\mathbf{x}_i] \bmod \Lambda + \mathbf{y}\Big] \bmod \Lambda &= \Big[\sum_i^K a_i\mathbf{x}_i + \mathbf{y}\Big] \bmod \Lambda \\ \Big(\sum_i^K a_i\mathbf{x}_{i_r} + \mathbf{y}\Big)_r &= \Big(\sum_i^K a_i\mathbf{x}_i + \mathbf{y}\Big)_r. \end{aligned} \tag{B.7}$$

Proof. Using the compact notation and applying theorem B.1 one obtains

$$\begin{aligned} \Big(\sum_i^K a_i\mathbf{x}_{i_r} + \mathbf{y}\Big)_r &= \Big(a_1\mathbf{x}_{1_r} + a_2\mathbf{x}_{2_r} + ... + a_K\mathbf{x}_{K_r} + \mathbf{y}\Big)_r \\ &= \Big(a_1(\mathbf{x}_1 - Q_\Lambda(\mathbf{x}_1)) + a_2(\mathbf{x}_2 - Q_\Lambda(\mathbf{x}_2)) + ... + a_K(\mathbf{x}_K - Q_\Lambda(\mathbf{x}_K)) + \mathbf{y}\Big)_r \\ &= \Big(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + ... + a_K\mathbf{x}_K - a_1Q_\Lambda(\mathbf{x}_1) - a_2Q_\Lambda(\mathbf{x}_2) - ... - a_KQ_\Lambda(\mathbf{x}_K) + \mathbf{y}\Big)_r \\ &= \Big(\sum_i^K a_i\mathbf{x}_i - \sum_i^K a_iQ_\Lambda(\mathbf{x}_i) + \mathbf{y}\Big)_r \\ &= \Big(\sum_i^K a_i\mathbf{x}_i + \mathbf{y}\Big)_r, \end{aligned} \tag{B.8}$$

since $\sum_i^K a_iQ_\Lambda(\mathbf{x}_i)$ is a lattice point according to lattice properties. □

Theorem B.5 ("General" distributive law for matrices)**.** For two matrices $\mathbf{X}$, $\mathbf{Y} \in \mathbb{R}^{K\times n}$ and any full-rank integer-valued matrix $\mathbf{A} \in \mathbb{Z}^{K\times K}$ one has that

$$\begin{aligned} [\mathbf{A}[\mathbf{X}] \bmod \Lambda + \mathbf{Y}] \bmod \Lambda &= [\mathbf{AX} + \mathbf{Y}] \bmod \Lambda \\ (\mathbf{AX}_r + \mathbf{Y})_r &= (\mathbf{AX} + \mathbf{Y})_r. \end{aligned} \tag{B.9}$$

Proof. Using the compact notation $(\mathbf{A}\mathbf{X}_r + \mathbf{Y})_r$ and by writing

$$\mathbf{X} \triangleq \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_K \end{bmatrix}, \mathbf{Y} \triangleq \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_K \end{bmatrix}$$

with $\mathbf{x}_i$, $\mathbf{y}_i$ being row vectors, one can also write

$$\mathbf{X}_r \triangleq [\mathbf{X}] \bmod \Lambda = \begin{bmatrix} \mathbf{x}_{1_r} \\ \mathbf{x}_{2_r} \\ \vdots \\ \mathbf{x}_{K_r} \end{bmatrix}, \mathbf{Y}_r \triangleq [\mathbf{Y}] \bmod \Lambda = \begin{bmatrix} \mathbf{y}_{1_r} \\ \mathbf{y}_{2_r} \\ \vdots \\ \mathbf{y}_{K_r} \end{bmatrix}.$$

Thus,

$$(\mathbf{A}\mathbf{X}_r + \mathbf{Y})_r = \left(\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1K} \\ a_{21} & a_{22} & \dots & a_{2K} \\ & & \vdots & \\ a_{K1} & a_{K2} & \dots & a_{KK} \end{bmatrix} \begin{bmatrix} \mathbf{x}_{1_r} \\ \mathbf{x}_{2_r} \\ \vdots \\ \mathbf{x}_{K_r} \end{bmatrix} + \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_K \end{bmatrix} \right)_r$$

$$= \begin{bmatrix} a_{11}\mathbf{x}_{1_r} + a_{12}\mathbf{x}_{2_r} + \ldots + a_{1K}\mathbf{x}_{K_r} + \mathbf{y}_1 \\ a_{21}\mathbf{x}_{1_r} + a_{22}\mathbf{x}_{2_r} + \ldots + a_{2K}\mathbf{x}_{K_r} + \mathbf{y}_2 \\ \vdots \\ a_{K1}\mathbf{x}_{1_r} + a_{K2}\mathbf{x}_{2_r} + \ldots + a_{KK}\mathbf{x}_{K_r} + \mathbf{y}_K \end{bmatrix}_r$$

$$= \begin{bmatrix} a_{11}\mathbf{x}_1 + a_{12}\mathbf{x}_2 + \ldots + a_{1K}\mathbf{x}_K + \mathbf{y}_1 \\ a_{21}\mathbf{x}_1 + a_{22}\mathbf{x}_2 + \ldots + a_{2K}\mathbf{x}_K + \mathbf{y}_2 \\ \vdots \\ a_{K1}\mathbf{x}_1 + a_{K2}\mathbf{x}_2 + \ldots + a_{KK}\mathbf{x}_K + \mathbf{y}_K \end{bmatrix}_r \tag{B.10}$$

$$= \left(\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1K} \\ a_{21} & a_{22} & \dots & a_{2K} \\ & & \vdots & \\ a_{K1} & a_{K2} & \dots & a_{KK} \end{bmatrix} \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_K \end{bmatrix} + \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_K \end{bmatrix} \right)_r$$

$$= (\mathbf{A}\mathbf{X} + \mathbf{Y})_r,$$

where theorem B.4 was applied to each row in the third transition. □

Lemma. For a matrix $\mathbf{X} \in \mathbb{R}^{K \times n}$ and any full-rank integer-valued matrix $\mathbf{A} \in \mathbb{Z}^{K \times K}$ one has that

$$\begin{aligned} [\mathbf{A}[\mathbf{X}] \bmod \Lambda] \bmod \Lambda &= [\mathbf{A}\mathbf{X}] \bmod \Lambda \\ (\mathbf{A}\mathbf{X}_r)_r &= (\mathbf{A}\mathbf{X})_r. \end{aligned} \tag{B.11}$$

Proof. Apply theorem B.5 with $\mathbf{Y}$ = [0]. □

Appendix C

Generalized Cauchy-Schwarz inequality

In this appendix the generalized Cauchy-Schwarz inequality is provided to support the derivation of an upper bound in chapter 5.

Definition C.1 (The 1-norm)**.** For a given column vector $\mathbf{x} \in \mathbb{R}^{K\times 1}$, its 1-norm is given by

$$\|\mathbf{x}\|_1 = \sum_{k=1}^{K} |x_k| \tag{C.1}$$

where $|\cdot|$ is the absolute value.

Definition C.2 (The inf-norm)**.** For a given column vector $\mathbf{x} \in \mathbb{R}^{K\times 1}$, its inf-norm is given by

$$\|\mathbf{x}\|_\infty = \max_{k=1,\dots,K} |x_k|. \tag{C.2}$$

Theorem C.1. For any two column vectors $\mathbf{u} \in \mathbb{R}^{K\times 1}$ and $\mathbf{v} \in \mathbb{R}^{K\times 1}$ one has that

$$\mathbf{u}^T\mathbf{v} \leq \|\mathbf{u}\|_1 \|\mathbf{v}\|_\infty . \tag{C.3}$$

Proof. One has that

$$\mathbf{u}^T\mathbf{v} \leq |\mathbf{u}^T\mathbf{v}|. \tag{C.4}$$

By expanding the second term and using the triangle inequality, one has that

$$\begin{aligned} |\mathbf{u}^T\mathbf{v}| &= |u_1v_1 + ... + u_Kv_K| \\ &\leq |u_1||v_1| + ... + |u_K||v_K|, \end{aligned} \tag{C.5}$$

and, using the definitions for 1-norm and inf-norm, one obtains

$$\begin{aligned} |u_1||v_1| + ... + |u_K||v_K| &\leq |u_1| \left\|\mathbf{v}\right\|_\infty + ... + |u_K| \left\|\mathbf{v}\right\|_\infty \\ &= \left\|\mathbf{u}\right\|_1 \left\|\mathbf{v}\right\|_\infty . \end{aligned} \tag{C.6}$$

□