# Maximum Likelihood Detection for the Linear MIMO Channel

JOAKIM JALDÉN


KTH Signals
Sensors and Systems

Licentiate Thesis
Stockholm, Sweden 2004

TRITA–S3–SB–0443
ISSN 1103–8039
ISRN KTH/SB/R - - 04/43 - - SE

Maximum Likelihood Detection for the Linear MIMO Channel

Signal Processing Laboratory
Department of Signals, Sensors and Systems
Royal Institute of Technology (KTH)
SE-100 44 Stockholm Sweden

Tel. +46 8 790 6000, Fax. +46 8 790 7260
http://www.s3.kth.se

# Abstract

In this thesis the problem of maximum likelihood (ML) detection for the linear multiple-input multiple-output (MIMO) channel is considered. The thesis investigates two algorithms previously proposed in the literature for implementing the ML detector, namely semidefinite relaxation and sphere decoding.

The first algorithm, semidefinite relaxation, is a suboptimal implementation of the ML detector meaning that it is not guaranteed to solve the maximum likelihood detection problem. Still, numerical evidence suggests that the performance of the semidefinite relaxation detector is close to that of the true ML detector. A contribution made in this thesis is to derive conditions under which the semidefinite relaxation estimate can be guaranteed to coincide with the ML estimate.

The second algorithm, the sphere decoder, can be used to solve the ML detection problem exactly. Numerical evidence has previously shown that the complexity of the sphere decoder is remarkably low for problems of moderate size. This has led to the widespread belief that the sphere decoder is of polynomial expected complexity. This is however unfortunately not true. Instead, in most scenarios encountered in digital communications, the expected complexity of the algorithm is exponential in the number of symbols jointly detected. However, for high signal to noise ratio the rate of exponential increase is small. In this thesis it is proved that for a large class of detection problems the expected complexity is lower bounded by an exponential function. Also, for the special case of an i.i.d. Rayleigh fading channel, an asymptotic analysis is presented which enables the computation of the expected complexity up to the linear term in the exponent.

# Acknowledgments

There are many people who have influenced and contributed to this work. This is the time to acknowledge their contributions.

First and foremost I whish to thank my advisor Professor Björn Ottersten who gave me the opportunity to work within this field and whose support and expertise has at many times proven invaluable. I also wish to thank my co-advisor Professor Mikael Skoglund for all his encouragement and help during my time with the department.

I wish to thank all my colleagues on the fourth floor for making this department a great place to work. I especially thank you for all our coffee-break discussions, both those related to work and even more so those not. I am truly grateful for being able to work with such talented people and for sharing your time and knowledge.

There are also some people who deserve special acknowledgments for their influence on this thesis. Apart from Professor Ottersten I wish to thank Cristoff Martin for introducing me to this topic and David Samuelsson for proofreading the thesis and pointing out my mistakes. I further wish to thank Dr. Wing-Kin Ma whose insightful feedback has inspired me to further develop much of the material presented herein. Last but not least I wish to thank Professor Lars Rasmussen for taking the time to act as opponent for the thesis.

Joakim Jaldén
Stockholm, September 2004

# Contents

# Chapter 1

# Introduction

A problem encountered in the design of receivers for digital communication systems is the detection of data from noisy measurements of the transmitted signals. In any realistic scenario the receiver is, due to the noise, bound to make occasional errors. Therefore, designing a receiver which has the property that this probability of error is minimal is appealing, both from a practical and a theoretical point of view.

Unfortunately, such designs tend to result in computationally complex receivers and for this reason they are often abandoned in favor of computationally simpler but suboptimal receivers. It is however well known that for many scenarios the gap in performance between suboptimal and the optimal receivers is substantial. This alone makes the optimal receivers interesting. Additionally, the decreasing cost of computation will result in computationally feasible optimal designs.

In this thesis, two near optimal designs are considered. These designs, or receiver algorithms, are in the communications literature commonly referred to as semidefinite relaxation and sphere decoding. The algorithms are also fundamentally different in the way with which they approach the detection problem. Both algorithms were originally developed in other fields to solve hard combinatorial problems which are conceptually different but mathematically similar to those encountered in the design of an optimal receiver. Various properties of the algorithms have previously been investigated, both in the context of the problems for which they were originally developed and in the context of digital communications. Still, many aspects of their behavior in the communications scenario are not yet fully understood.

The contribution of this work is to further increase the understanding of these algorithms in the context of digital communications. Depending on the specific algorithm, different aspects will be treated.

## 1.1 Historical Overview

The maximum likelihood (ML) detection problem for the linear multiple-input multiple-output (MIMO) channel was first investigated in the context of CDMA after it was shown that an optimum detector offered a significant gain in performance over conventional symbol by symbol detectors [Ver86]. In the context of CDMA the problem of optimal detection is usually referred to as optimal multiuser detection (MUD) since in this scenario the ML detection problem corresponds to the simultaneous detection of several users' symbols in the presence of multiple access interference. More recently, similar detection problems have also been addressed when studying the joint detection of several symbols transmitted over a multiple antenna fading channel.

The ML detection problem is known to be NP-hard [Ver89]. This implies that, unless there is some additional underlying structure in the problem considered, no known algorithms for it's solution are of polynomial complexity in the number of symbols jointly detected. For this reason a large number of suboptimal, but computationally less complex, receivers have been considered in the literature.

The most common class of suboptimum detectors is the class of linear detectors [LV89]. These detectors apply a linear transformation to the received symbols prior to performing symbol by symbol decisions. The linear detectors include the zero-forcing (ZF) or decorrelating detector and the minimum mean square error (MMSE) detector [XSR90]. A more advanced class of detectors is given by the class of decision feedback (DF) detectors. These detectors make decisions on one symbol at the time and then subtract the contribution of this symbol on the remaining symbols prior to the next detection [Due99, Due95]. In these detectors, the order in which the symbols are detected will strongly affect the performance of the detector and thus various ordering strategies have been considered in the literature [Var99]. Other detectors of interest are the multistage detectors [VA90, VA91] and the group detectors [Var95]. Tutorials on the topic of multiuser detection are given in [Ver93, DHZ95], see also [Ver98].

Typically, there is a tradeoff between computational complexity and accuracy of the above detectors. The linear detectors which are also

the fastest have in general worse performance than the decision feedback and group detectors which are computationally more complex. A recent analysis of the complexity performance tradeoff of several detections techniques is found in [HLP+04]. Also, as shall be seen herein, the relative performance of the detectors may vary with system parameters such as for instance the signal to noise ratio.

As the cost of computation has decreased interest has shifted towards implementations of the optimal detector. As is stated in the introduction, this thesis considers two algorithms which have been previously proposed for the solution, or at least an approximate solution, of the ML detection problem. The first algorithm, or strategy, is referred to as semidefinite relaxation (SDR) and has previously been used to approximate the solution of hard combinatorial problems, see [VB96] and references therein. It was introduced into the field of digital communications in the context of CDMA [TR01, MDW+02]. The second algorithm, now commonly referred to as the sphere decoder[1], was initially developed for finding vectors of short length in arbitrary lattices [Poh81, FP85]. Since it's introduction into the field of digital communications it has found a wide variety of applications, both in the context of CDMA and for the multiple antenna channel, see e.g. [VB99, DGC03].

## 1.2 Outline and Contributions

This section outlines the chapters of this thesis. It also highlights the scientific contributions which are presented herein. It should be noted that the focus of this thesis is not on the introduction of new methods to solve the detection problem but rather the analysis of methods which have previously been suggested in the literature.

### 1.2.1 Chapter 2

This chapter provides a common framework for the rest of the thesis. The model for the linear multiple-input multiple-output (MIMO) channel is presented. A few motivating examples of systems which have previously been studied in the literature and which may be modeled as linear MIMO channels are given.

[1]The name sphere decoder is due to a geometric visualization of the algorithm where the constellation points belonging to a high dimensional sphere are considered in the detection process.

Based on the given channel model the mathematical formulation of the ML detector is derived. This forms a common basis for the algorithms in Chapters 3 and 4. Also, formal definitions of the concepts of polynomial and exponential complexity are given.

### 1.2.2 Chapter 3

In this chapter the semidefinite relaxation approach to near ML detection for the linear MIMO channel is considered. In particular, conditions under which the semidefinite relaxation estimate coincides with the true ML estimate are derived. Part of the material in this chapter has been previously published in

[**JMO03**] J. Jaldén, C. Martin and B. Ottersten. Semidefinite Programming for Detection in Linear Systems – Optimality Conditions and Space-Time Decoding. In *Proc. IEEE ICASSP'03*, April 2003.

The content of Section 3.2.1 is previously unpublished and is due to a suggestion by Dr. W.-K. Ma. The material has however recently been submitted as

[**JOM04**] J. Jaldén, B. Ottersten and W.-K. Ma. Reducing the average complexity of ML detection using semidefinite relaxation. Submitted to *IEEE ICASSP'05*, September 2004.

The highlights and contribution of this chapter are

- Theorem 3.1 which characterize when the semidefinite relaxation solution coincides with the ML solution.
- Section 3.2.1 which highlights a practical application of Theorem 3.1.

### 1.2.3 Chapter 4

This chapter reviews the sphere decoding algorithm and it's use to ML detection. Sphere decoding has previously been thought to have polynomial expected complexity. One of the contributions of this chapter is to show that, under conditions applicable to a large class of detection problems, this notion is incorrect. Part of the material of this section has been previously published in

[**JO04a**] J. Jaldén and B. Ottersten. An Exponential Lower Bound on the Expected Complexity of Sphere Decoding. In *Proc. IEEE ICASSP'04*, May 2004.

[**JO04b**] J. Jaldén and B. Ottersten. On the expected complexity of sphere decoding in digital communications. To appear in *IEEE Transactions on Signal Processing*.

The highlights and scientific contributions of this chapter are

- Lemma 4.2 which provides a probabilistic reformulation of the sphere decoder complexity and thus enables complexity analysis by the use of tools from probability theory.
- Theorems 4.1 and 4.3 which establish that the expected complexity of the sphere decoder is exponential for the vast majority of scenarios previously considered in the literature.
- Theorems 4.4 and 4.7 which together with Section 4.3.2 offer a constructive way to compute the exact exponential rate for the expected complexity of the sphere decoder in the case of the i.i.d. Rayleigh fading channel.

### 1.2.4 Chapter 5

This chapter illustrates some properties of the two algorithms by the use of simulations. The material of this chapter is not previously published although investigation of this type have been considered by other authors. It is not within the scope of this thesis to present an extensive investigation into the performance of the algorithms in various scenarios. The simulations presented in this chapter are included simply to motivate some of the statements made in the previous chapters and illustrate the typical behavior of the algorithms.

## 1.3 Notation

The following notation will be used throughout the thesis. Plain letters, e.g. $a$ and $A$, are used for scalars. Boldface letters are used for vectors and matrices, e.g. $\mathbf{x}$ is a column vector and $\mathbf{X}$ is a matrix. Calligraphic upper case letters, e.g. $\mathcal{A}$, are used to denote sets. The set notation will also be used to denote probabilistic events. Also, no notational distinction will be made between random variables and their realizations.

| | |
|---|---|
| $\mathbf{x}^{\mathrm{T}}$, $\mathbf{X}^{\mathrm{T}}$ | The transpose of a vector, $\mathbf{x}$, or matrix, $\mathbf{X}$. |
| $\mathbf{x}^{\mathrm{H}}$, $\mathbf{X}^{\mathrm{H}}$ | The Hermitian or conjugate transpose of a vector, $\mathbf{x}$, or matrix, $\mathbf{X}$. |
| $\mathbf{X}^{\dagger}$ | Moore-Penrose generalized inverse [HJ85]. |
| $\mathbf{x}_{\iota_k}$ | The vector given by the $k$ last components of $\mathbf{x}$, i.e. $\mathbf{x} = [x_1 \dots\ x_m]^{\mathrm{T}} \Rightarrow \mathbf{x}_{\iota_k} = [x_{m-k+1} \dots\ x_m]^{\mathrm{T}}$ |
| $\|\mathbf{x}\|$ | The Euclidian norm of a vector $\mathbf{x}$, i.e. $\|\mathbf{x}\| = \sqrt{\mathbf{x}^{\mathrm{H}}\mathbf{x}}$. |
| $\mathbf{X} \circ \mathbf{Y}$ | Elementwise product of matrices. |
| $\mathrm{Rank}(\mathbf{X})$ | The rank of a matrix, $\mathbf{X}$, i.e. the number of linearly independent rows or columns. |
| $\mathrm{Range}(\mathbf{X})$ | The range of $\mathbf{X}$, i.e. the linear subspace spanned by the columns of $\mathbf{X}$. |
| $\mathrm{Tr}(\mathbf{X})$ | Trace of a matrix, i.e. the sum of the diagonal elements. |
| $\mathrm{diag}(\mathbf{X})$ | The column vector with the diagonal elements of $\mathbf{X}$. |
| $\mathrm{Diag}(\mathbf{x})$ | The diagonal matrix with elements given by $\mathbf{x}$. |
| $\mathcal{A} \times \mathcal{B}$ | Cartesian product of $\mathcal{A}$ and $\mathcal{B}$, i.e. $\mathcal{A} \times \mathcal{B} = \{(a, b) \mid a \in \mathcal{A},\ b \in \mathcal{B}\}$. |
| $\mathcal{A}^m$ | $m$:th Cartesian product, $\mathcal{A} \times \mathcal{A} \times \ldots \times \mathcal{A}$. |
| $\lvert\mathcal{A}\rvert$ | The cardinality or size of a finite set $\mathcal{A}$, i.e. the number of elements for finite sets. |
| $\mathcal{A}^o$ | Interior of a set $\mathcal{A}$ with respect to the Euclidian norm [Rud96]. |
| $\bar{\mathcal{A}}$ | The closure of a set $\mathcal{A}$ with respect to the Euclidian norm [Rud96]. |
| $\mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{N}$ | The sets of real, complex, integer, and natural numbers. |
| $\Re(a)$ | The real part of a complex number $a$. |
| $\Im(a)$ | The imaginary part of a complex number $a$. |
| $\{a_k\}_{k=1}^{\infty}$ | A sequence of numbers or random variables. |
| $\lim_{k\to\infty} a_k$ | Limit of a sequence $\{a_k\}_{k=1}^{\infty}$. |
| $\limsup_{k\to\infty} a_k$ | Limit superior of a sequence $\{a_k\}_{k=1}^{\infty}$. |
| $\liminf_{k\to\infty} a_k$ | Limit inferior of a sequence $\{a_k\}_{k=1}^{\infty}$. |
| $\sup_{a\in\mathcal{A}} f(a)$ | Supremum of $f(a)$ over $\mathcal{A}$. |
| $\inf_{a\in\mathcal{A}} f(a)$ | Infimum of $f(a)$ over $\mathcal{A}$. |
| a.s. | Almost surely, i.e. with probability one. |
| $\mathrm{P}(\mathcal{A})$ | Probability of $\mathcal{A}$. |
| $\mathrm{P}(\mathcal{A}\lvert\mathcal{B})$ | Probability of $\mathcal{A}$ given $\mathcal{B}$. |

| | |
|---|---|
| $\mathrm{E}\{a\}$ | Expected value of $a$. |
| $\mathrm{E}\{a\|\mathcal{A}\}$ | Conditional expectation of $a$ given $\mathcal{A}$. |
| $\mathcal{U}(\mathcal{A})$ | Uniform distribution over $\mathcal{A}$. |
| $\mathcal{N}_C(\mu, \sigma^2)$ | Complex Gaussian distribution with mean $\mu$ and variance $\sigma^2$. |
| $\triangleq$ | Equal by definition. |
| $\doteq$ | Equal to the first order in the exponent. |
| ln | Natural logarithm. |
| $\log_b$ | Base $b$ logarithm. |
| $\lceil a \rceil$ | Ceil function, i.e. $\lceil a \rceil = b$ where $b \in \mathbb{Z}$ is the smallest integer such that $a \leq b$. |
| $\lfloor a \rfloor$ | Floor function, i.e. $\lfloor a \rfloor = b$ where $b \in \mathbb{Z}$ is the largest integer such that $a \geq b$. |

## 1.4 Abbreviations

**BER** Bit Error Rate

**BPSK** Binary Phase Shift Keying

**CDMA** Code Division Multiple Access

**DF** Decision Feedback

**FIR** Finite Impulse Responce

**ISI** Intersymbol Interference

**KKT** Karush-Kuhn-Tucker (optimality conditions)

**MIMO** Multiple-Input Multiple-Output

**ML** Maximum Likelihood

**MMSE** Minimum Mean Square Error

**MUD** Multiuser detection

**NP** Nondeterministic Polynomial

**QPSK** Quadrature Phase Shift Keying

**SD** Sphere Decoder

**SDR** Semidefinite relaxation

**SNR** Signal to Noise Ratio

**STBC** Space-Time Block Code

**ZF** Zero-Forcing

# Chapter 2

# The Maximum Likelihood Detection Problem

This chapter serves the purpose of introducing some central elements of this work, i.e. the linear multiple input, multiple output (MIMO) channel and the mathematical formulation of the corresponding maximum likelihood (ML) detector. This provides a common framework for the material of Chapters 3 to 5.

Additionally, the concept of algorithm complexity will be introduced. The definitions given in this chapter will play a fundamental role in the analysis of the sphere decoder in Chapter 4 and also be useful for the evaluation of the semidefinite relaxation in Chapter 3.

## 2.1 System Models

The system model considered herein is widely used to model various digital communication systems. As the same model may be used to model a variety of different system it is convenient to first treat it in an abstract form which does not make any explicit assumptions about an underlying physical model. The material of the following chapters is based on this abstract model and is therefore applicable to several different scenarios depending on which physical meaning the quantities of the abstract model

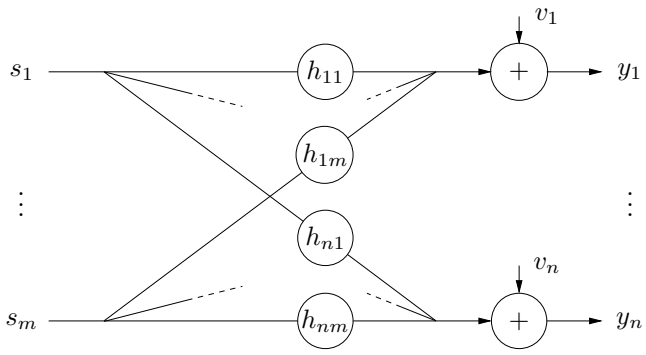


**Figure 2.1:** A linear MIMO channel with $m$ inputs and $n$ outputs.

are given. Examples of a few of the, in the communications literature, common scenarios to with the linear MIMO model is applicable are then given in Section 2.1.2.

### 2.1.1 The Linear MIMO Channel

As stated in the introduction, a key element of this work is the linear MIMO channel which is illustrated in Figure 2.1. The premise is that a transmitter simultaneously transmits $m$ *symbols*, $s_1, \ldots, s_m$, from a finite alphabet or *constellation* $\mathcal{S} \subset \mathbb{C}$. At the receiver $n$ signals, $y_1, \ldots, y_n$, are received, each signal being a linear combination of the $m$ input symbols plus an additive noise component. Depending on the context in which the model is used it may be more natural to view the transmitter and receiver as several transmitters or receivers respectively. A constraint which will be placed on the receivers in this case is that there is a possibility of cooperations. However, since only receiver design is treated herein, there is no need to impose such a constraint on the transmitters. It will however, unless otherwise stated, be assumed that the number of received signals, $n$, exceeds the number of transmitted symbols, i.e. that $n \geq m$. This assumption will later have the consequence that systems of equations, required to be solved in the detection process, are not under determined. Although a common assumption in the literature, this may in some scenarios limit the applicability of the derived results.

The linear MIMO channel is commonly, and conveniently, modeled

on matrix form as

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{v} \tag{2.1}$$

where $\mathbf{H} \in \mathbb{C}^{n \times m}$ is referred to as the *channel matrix* and $\mathbf{v} \in \mathbb{C}^n$ is the additive *noise*. The vectors $\mathbf{y} \in \mathbb{C}^n$ and $\mathbf{s} \in \mathcal{S}^m$ are the received signals and transmitted symbols respectively. The interpretation of (2.1) is typically that some superposition the symbols, $\mathbf{s}$, given by the channel matrix, $\mathbf{H}$, are measured at the receiver as $\mathbf{y}$ where $\mathbf{v}$ models the measurement noise. While the specific structure of the channel matrix is given by the specific scenario under consideration it will herein be assumed that $\mathbf{H}$ is known, i.e. has been previously estimated, by the receiver. Thus, the objective of the receiver will be to estimate $\mathbf{s}$ from the pair $(\mathbf{y}, \mathbf{H})$. In the analysis to follow $\mathbf{H}$ is generally treated as a random quantity. However, in all scenarios where no explicit distribution is assigned to $\mathbf{H}$, the channel matrix may be considered a deterministic quantity by simply considering a degenerate distribution.

The symbols transmitted are modeled as i.i.d. random variables which are uniformly distributed over the constellation alphabet, $\mathcal{S}$. It is assumed that the constellation is centered at zero, i.e.

$$\mathrm{E}\{\mathbf{s}\} = \mathbf{0}$$

under the i.i.d. assumption on $\mathbf{s}$. Note that this occurs at no loss of generality since any nonzero mean of $\mathbf{s}$, and consequently $\mathbf{y}$, may be removed prior to detection without any loss in performance. Also, designing a communications system with a nonzero mean would in most scenarios require an increased transmit power and thus, the assumption is usually satisfied in practice as well.

The noise is modeled as zero mean, circularly symmetric complex Gaussian, with variance $\sigma^2$ and is assumed uncorrelated between components. The Gaussian assumption is usually motivated by the notion that the noise is made up of several contributing components and is thus approximately Gaussian due to the central limit theorem. The ability to correctly detect the transmitted symbols, $\mathbf{s}$, is affected by the ratio of the signal strength and the noise power. This ratio is called the *signal to noise ratio* (SNR) and is herein defined as

$$\rho \triangleq \frac{\mathrm{E}\left\{\|\mathbf{H}\mathbf{s}\|^2\right\}}{\mathrm{E}\left\{\|\Pi_{\mathbf{H}}\mathbf{v}\|^2\right\}} \tag{2.2}$$

where

$$\Pi_{\mathbf{H}} \triangleq \mathbf{H}(\mathbf{H}^{\mathrm{H}}\mathbf{H})^{\dagger}\mathbf{H}^{\mathrm{H}}$$

is the projection matrix for the projection onto the space spanned by the columns of $\mathbf{H}$. The reason for including the projection of the noise onto the columns of $\mathbf{H}$ is that the part of the noise orthogonal to $\mathbf{H}$ does not affect the ability to correctly detect $\mathbf{s}$ and is thus irrelevant to the detection problem. Note that in the special case where $m = n$ and where $\mathbf{H}$ is full rank with probability 1, (2.2) reduce to the perhaps more familiar expression

$$\rho = \frac{\mathrm{E}\left\{\|\mathbf{Hs}\|^2\right\}}{\mathrm{E}\left\{\|\mathbf{v}\|^2\right\}}.$$

### 2.1.2 Examples of Linear MIMO Channels

This section gives a few important examples of where the linear MIMO channel model is applicable. The examples are intended to motivate the use of the model given in (2.1) and are by no means the only systems which can be modeled on this form. Application of the algorithms of Chapters 3 and 4 has been previously considered in the literature for most of the examples below.

#### The Multiple Antenna Channel

The perhaps most straightforward application of the linear MIMO model is the synchronous, base-band, time-discrete, frequency-flat multiple antenna channel. In this scenario the transmitter is equipped with $m$ antennas and simultaneously transmits one symbol per antenna. Alternatively, as noted in the introduction, there may be $m$ single antenna transmitters. The receiver is equipped with $n$ antennas and receive the the signals $y_1$ to $y_n$, one per antenna. The coefficients of the channel matrix, $h_{ij}$, are in this case interpreted as the complex base-band equivalent gains from transmit antenna $j$ to receive antenna $i$.

An important special case of the multiple antenna channel, the i.i.d. Rayleigh fading channel, is treated in Section 2.1.3.

#### Linear Dispersive STBC's

Under the assumption that the channel gains of the multiple antenna channel stay constant over $L$ transmissions the channel can be conveniently modeled on matrix form as

$$\mathbf{Y} = \mathbf{HS} + \mathbf{V}$$

where $\mathbf{Y} \in \mathbb{C}^{n\times L}$, $\mathbf{S} \in \mathbb{C}^{m\times L}$, and $\mathbf{V} \in \mathbb{C}^{n\times L}$. Here, the $ij$:th element of $\mathbf{S}$ represents the symbol transmitted from antenna $i$ at time $j$. Similarly, the $ij$:th element of $\mathbf{Y}$ is the signal received at antenna $i$ at time $j$. In a linear dispersive space time block coding scheme [HH02], the transmitted matrix symbol, $\mathbf{S}$, is chosen as

$$\mathbf{S} = \sum_{i=1}^{m} \mathbf{C}_i s_i$$

where $\mathbf{C}_i$ are complex matrices typically referred to as the dispersion matrices and $s_i \in \mathcal{S}$ are the transmitted data symbols. By employing such a linear block code the received symbols $\mathbf{Y}$ are given by

$$\mathbf{Y} = \sum_{i=1}^{m} \mathbf{H}\mathbf{C}_i s_i + \mathbf{V}.$$

Note that this system is also linear in the transmitted symbols $s_i$ and by stacking the columns of $\mathbf{Y}$ into a vector this system can be written on the form of (2.1).

### The FIR Channel

Consider a single antenna time-discrete finite impulse response (FIR) channel where the channel output at time $k$, $y(k)$, is given by

$$y(k) = h(k) \star x(k) + v(k) \triangleq \sum_{l=0}^{L} h(l)s(k-l) + v(k)$$

where $s(k)$ is the transmitted symbol at time $k$, $h(l)$ is the channel impulse response, and $v(k)$ is an additive noise term. Assume that the channel impulse response, $h(l)$ is zero for $l \neq [0, L]$ and that a burst of $K+1$ symbols, $s(0), \ldots, s(K)$, is transmitted. Then this system may be written on matrix form as

$$\begin{bmatrix} y(0) \\ y(1) \\ \vdots \\ y(K) \end{bmatrix} = \begin{bmatrix} h(0) & & \cdots & & 0 \\ h(1) & h(0) & & & \\ \vdots & & & & \vdots \\ 0 & \cdots & h(L) & \cdots & h(0) \end{bmatrix} \begin{bmatrix} s(0) \\ s(1) \\ \vdots \\ s(K) \end{bmatrix} + \begin{bmatrix} v(0) \\ v(1) \\ \vdots \\ v(K) \end{bmatrix}$$

which is on the form of (2.1). However, in some cases, particularly when $L$ is small, other algorithms may be more efficient than those considered herein due to the structure of $\mathbf{H}$.

### CDMA

In a synchronous code division multiple access (CDMA) system several users communicate simultaneously over a shared channel. User number $j$ is distinguished by a unique signature waveform $p_j(t)$. The received, time continuous, signal is given by

$$x(t) = \sum_{j=1}^{m} p_j(t)s_j + w(t)$$

where $w(t)$ is a white Gaussian noise process and $s_j$ is the information symbol transmitted by the $j$:th user. It was shown in [Ver86] that the optimal detector in this scenario consists of a bank of matched filters, one for each users' signature, followed by a discrete time multiuser detector. Let $x_i$ be the output of the $i$:th matched filter, i.e.

$$x_i = \int_{\mathcal{T}} p_k^*(t)x(t)dt = \sum_{i=1}^{m} r_{ij}s_j + w_i$$

where $\mathcal{T}$ is the symbol duration,

$$r_{ij} = \int_{\mathcal{T}} p_i^*(t)p_j(t)dt$$

and

$$w_i = \int_{\mathcal{T}} p_i^*(t)w(t)dt.$$

As in the case of the multiple antenna channel this system can also be written on matrix form, i.e.

$$\mathbf{x} = \mathbf{R}\mathbf{s} + \mathbf{w},$$

with the difference that in this case the noise, $\mathbf{w}$, is correlated according to

$$\mathrm{E}\left\{\mathbf{w}\mathbf{w}^{\mathrm{H}}\right\} = \mathbf{R}.$$

This can however be accounted for by whitening the signal with the inverse of a square root factor, $\mathbf{R}^{-1/2}$, of the correlation matrix, i.e.

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{v}$$

where $\mathbf{y} \triangleq \mathbf{R}^{-1/2}\mathbf{x}$, $\mathbf{H} = \mathbf{R}^{1/2}$ and where $\mathbf{v}$ is now white Gaussan noise. Thus, the CDMA system can be written on the form of (2.1).

This CDMA model may be made more interesting by incorporating for example different transmission powers for the users while still being on the form of (2.1). Both the CDMA model and the multiple antenna model can also be further extended to model a block of transmitted symbols under the influence of inter-symbol interference (ISI) by rewriting the system in a similar fashion as was done with the finite impulse response channel.

### 2.1.3 The Rayleigh Fading Model

A linear MIMO channel which is common in the literature is the i.i.d. Rayleigh fading channel. This channel is a special case of the multiple antenna channel where the elements of the channel matrix, $\mathbf{H}$, are distributed according to an i.i.d. complex, circularly symmetric Gaussian distribution. This channel model has a few properties which makes it especially appealing. First, it tends to be a good model for many fading multiple antenna channels. Secondly, in many cases it's mathematical simplicity enables analytical evaluation of systems where it is used to model the channel.

The i.i.d. Rayleigh fading channel has been extensively investigated in the literature, both for finite $m$, e.g. [Tel99, Gra02], and asymptotically in $m$, e.g. [BTT02]. Herein, the i.i.d. Rayleigh fading model will be used in the asymptotic analysis of Section 4.3 and for the numerical examples in Chapter 5.

## 2.2 The Maximum Likelihood Detector

The object of the receiver is as previously stated to obtain an estimate of the message, $\mathbf{s}$, from the given data in $\mathbf{y}$ and $\mathbf{H}$. There are a wide variety of techniques for doing this but as stated in the introduction this work will only be concerned with the *maximum likelihood* (ML) detector and approximation thereof. The ML detector has the desirable property that, under the statistical assumptions on $\mathbf{s}$ given in Section 2.1.1, it minimizes the probability of error,

$$P_e \triangleq \mathrm{P}\left(\mathbf{s} \neq \hat{\mathbf{s}}\right).$$

Note that minimizing the probability of error is equivalent to maximizing the probability of correctly estimating $\mathbf{s}$, i.e.

$$\mathrm{P}\left(\mathbf{s} = \hat{\mathbf{s}} | \mathbf{y}, \mathbf{H}\right). \tag{2.3}$$

To derive the criterion function commonly used in the receiver note that the probability of equation (2.3) may alternatively be written as [Pro95]

$$\mathrm{P}\left(\mathbf{s}=\hat{\mathbf{s}}|\mathbf{y},\mathbf{H}\right)=\frac{\mathrm{P}\left(\mathbf{s}=\hat{\mathbf{s}}\right)f_{\mathbf{y}|\mathbf{s},\mathbf{H}}(\mathbf{y}|\mathbf{s}=\hat{\mathbf{s}},\mathbf{H})}{f_{\mathbf{y}|\mathbf{H}}(\mathbf{y}|\mathbf{H})}$$

where $f_{\mathbf{y}|\mathbf{H}}$ and $f_{\mathbf{y}|\mathbf{s},\mathbf{H}}$ are the conditional probability density functions of $\mathbf{y}$ given $\mathbf{H}$ and $(\mathbf{s},\mathbf{H})$ respectively. Since neither $\mathrm{P}\left(\mathbf{s}=\hat{\mathbf{s}}\right)$ nor $f_{\mathbf{y}|\mathbf{H}}(\mathbf{y}|\mathbf{H})$ depends on $\hat{\mathbf{s}}$ the criterion of (2.3) is maximized by the $\hat{\mathbf{s}}$ which maximizes

$$f_{\mathbf{y}|\mathbf{s},\mathbf{H}}(\mathbf{y}|\mathbf{s}=\hat{\mathbf{s}},\mathbf{H}) \tag{2.4}$$

Equation (2.4) is referred to as the ML criterion and the detector given by

$$\hat{\mathbf{s}}_{\mathrm{ML}}=\underset{\hat{\mathbf{s}}\in\mathcal{S}^m}{\operatorname{argmax}}\ f_{\mathbf{y}|\mathbf{s},\mathbf{H}}(\mathbf{y}|\mathbf{s}=\hat{\mathbf{s}},\mathbf{H}) \tag{2.5}$$

is referred to as the ML detector. Note that the ML detector is always given by (2.5) even in the case where $\mathrm{P}\left(\mathbf{s}=\hat{\mathbf{s}}\right)$ is not constant, i.e. when symbols are transmitted with nonuniform probabilities, but that in this case it is not optimal in the sense that it maximize the probability of obtaining the transmitted message. Equation (2.5) may be further simplified by applying the model of (2.1) to obtain

$$f_{\mathbf{y}|\mathbf{s},\mathbf{H}}(\mathbf{y}|\mathbf{s}=\hat{\mathbf{s}},\mathbf{H})=f_{\mathbf{v}}(\mathbf{y}-\mathbf{H}\hat{\mathbf{s}}).$$

Further, note that the probability density of the white Gaussian noise, $\mathbf{v}$, is given by

$$f_{\mathbf{v}}(\mathbf{v})=\frac{1}{(\pi\sigma^2)^n}e^{-\frac{1}{\sigma^2}\|\mathbf{v}\|^2}.$$

Thus, the likelihood of $\hat{\mathbf{s}}$ is obtained by substituting $\mathbf{v}$ with $\hat{\mathbf{v}}\triangleq\mathbf{y}-\mathbf{H}\hat{\mathbf{s}}$ in the above. By observing that $f_{\mathbf{y}|\mathbf{s},\mathbf{H}}$ is maximized by minimizing $\|\hat{\mathbf{v}}\|^2$ the ML estimate of $\mathbf{s}$, i.e. $\hat{\mathbf{s}}_{\mathrm{ML}}$, is given by

$$\hat{\mathbf{s}}_{\mathrm{ML}}=\underset{\hat{\mathbf{s}}\in\mathcal{S}^m}{\operatorname{argmin}}\ \|\mathbf{y}-\mathbf{H}\hat{\mathbf{s}}\|^2. \tag{2.6}$$

Thus, the ML detector chooses the message $\hat{\mathbf{s}}$ which yields the smallest distance between the received vector, $\mathbf{y}$, and hypothesized message, $\mathbf{H}\hat{\mathbf{s}}$.

The ML detector of (2.6) represents a discrete optimization problem over $|\mathcal{S}|^m$ candidate vectors $\hat{\mathbf{s}}\in\mathcal{S}^m$. Unfortunately, such problems are in general hard to solve and it has been shown that the problem of (2.6) for general $\mathbf{y}$ and $\mathbf{H}$ is NP-hard [Ver89]. However, for moderate problem sizes, $m$, there are several efficient algorithms available for the solution or approximation of (2.6) and as previously mentioned the primary topic of this thesis is the study of two such algorithms.

## 2.3 Computational Complexity

When analyzing an algorithm it is useful to establish how the computational complexity varies with parameters such as the size, $m$, or the SNR, $\rho$. Herein, focus will be on the dependence on $m$. An investigation into how the complexity depends on $m$ will yield useful information about when a specific algorithm is well suited. Depending on the physical interpretation of the abstract model, this may include how large dispersion matrices may be used in an LD scheme or how many users that can be accommodated in a CDMA system.

However, a direct study of how much time an algorithm requires to solve a specific problem of size, $m$, will generally depend on the particular hardware on which the algorithm is implemented and is therefore limited in it's scope. For this reason it is more common to instead study how the complexity varies with $m$ and to classify the algorithm based on this behavior. The complexity classes relevant to this work are treated in the following section.

### 2.3.1 Polynomial and Exponential Complexity

As the concept of algorithm complexity will play a fundamental role in this work it is useful to give definitions of what is meant by statements such as polynomial and exponential complexity. To this end, consider the following definitions [AHU74, NW88].

**Definition 2.1.** *A function $f(m)$ is said to be in $O(g(m))$ if there exist constants $c$ and $M$ such that $f(m) \leq cg(m)$ for all $m \geq M$.*

**Definition 2.2.** *A function $f(m)$ is said to be in $\Omega(g(m))$ if there exist constants $c$ and $M$ such that $f(m) \geq cg(m)$ for all $m \geq M$.*

**Definition 2.3.** *A function $f(m)$ is said to grow polynomially if there exists a constant $a \geq 0$ such that $f(m) \in O(m^a)$.*

**Definition 2.4.** *A function $f(m)$ is said to grow exponentially if there exist constants $a > 1$ and $b > 1$ such that $f(m) \in \Omega(a^m) \cap O(b^m)$.*

By the definitions it can be seen that a function which grows polynomially will always, for some large enough $m$, be smaller than an exponentially growing function. The definitions do however not give any direct hint as to how large this $m$ needs to be and are thus asymptotic in nature. Why exactly the definitions must be formulated in this way is further elaborated on in Section 2.3.2.

To introduce the notion of complexity classes note that the detection algorithms considered herein can be viewed as sequences of functions $\{\varphi_m\}_{m=1}^{\infty}$

$$\varphi_m : \mathcal{A}_m \mapsto \mathcal{B}_m$$

which given some input $a \in \mathcal{A}_m$ of size $m$ produce an output $b \in \mathcal{B}_m$. Specifically, for the algorithms considered herein the input will be the pair $(\mathbf{y}, \mathbf{H}) \in \mathbb{C}^n \times \mathbb{C}^{n \times m}$ and the output an estimate $\hat{\mathbf{s}} \in \mathcal{S}^m$. The size of an input will always be taken to mean the number of symbols, $m$, which are jointly detected in (2.6). The computation of $\varphi_m$ will require a number of basic operations such as additions, multiplications etc., the number of which typically depend on the particular input $a$. Let $\vartheta_m(a)$ be the number of operations required for the input $a \in \mathcal{A}_m$, i.e.

$$\vartheta_m : \mathcal{A}_m \mapsto \mathbb{N}.$$

The complexity of the algorithm, $\Phi(m)$, is then defined as

$$\Phi(m) \triangleq \sup_{a \in \mathcal{A}_m} \vartheta_m(a)$$

and the algorithm is said to be of polynomial or exponential complexity if $\Phi(m)$ grows polynomially or exponentially, respectively. However, in some cases the complexity of the algorithm does not describe the usual behavior of the algorithm. Thus, whenever there is some sequence of probability measure, $\{\mu_m\}_{m=1}^{\infty}$, associated with the inputs $a \in \mathcal{A}_m$ the expected [AHU74], or average, complexity can be defined as

$$\Psi(m) \triangleq \mathrm{E}\left\{\vartheta_m(a)\right\}$$

where the expected value is computed with respect to the measure $\mu_m$. Thus, an algorithm is said to be of polynomial or exponential expected complexity if $\Psi(m)$ grows polynomially or exponentially respectively. In general the measure $\mu_m$ will not be given explicitly but implicitly by the assumptions and models used when analyzing the algorithms. It is however important to realize that the existence of such a probability measure is essential to the definition of expected complexity. Also, remember that while $\Phi(m)$ and $\Psi(m)$ are referred to as the complexity and expected complexity of the algorithms any statement about polynomial and exponential always refer to the asymptotic nature of $\Phi(m)$ and $\Psi(m)$. A note of caution is also that these definitions ultimately depend on the definition of the basic operation. However, to give a stringent definition of this

concept requires a much more elaborate framework and is not within the scope of this thesis.

The following observations will prove useful in the analysis to come. A function $f(m)$ grows polynomially if and only if

$$\limsup_{m\to\infty} \frac{\ln f(m)}{\ln m} < \infty.$$

Similarly, a function grows exponentially if and only if

$$\liminf_{m\to\infty} \frac{1}{m} \ln f(m) > 0$$

and

$$\limsup_{m\to\infty} \frac{1}{m} \ln f(m) < \infty.$$

Also, note that an algorithm can not be of polynomial or exponential complexity at the same time. It is however possible for an algorithm to be of exponential complexity but of polynomial *expected* complexity.

### 2.3.2 Finite Size Analysis

Recently, there has in the communications literature been statements suggesting that various algorithms are of polynomial complexity for some given *finite* range of $m$, see e.g. [HV03, HB03]. This is in conflict with Definition 2.3 which require a polynomial bound which holds for arbitrary large $m$. At first glance the difference may seem as merely a mathematical curiosity but a closer inspection show that arbitrary large $m$ are indeed necessary to be able to make the notion of polynomial complexity meaningful. Similarly, any attempt to redefine the definition of polynomial complexity to hold for a finite range of $m$ is bound to introduce inconsistencies.

Intuition may suggest that it is sufficient that the complexity behave like a polynomial function in the range of $m$ which are of practical interest. The problem with such intuition is that it is not at all clear how exactly a polynomial function behaves. By the Stone-Weierstrass theorem [Rud96] it is known that any continuous function on a closed and bounded interval may be arbitrary well approximated by a polynomial. Thus, any continuous function can be said to behave like a polynomial or vice verse. This implies that almost all algorithms, including the full search solution of (2.6), have a complexity which is well approximated by

a polynomial function if the size, $m$, is restricted to some finite range. In short, by restricting the analysis to a finite range of $m$ will also render the notion of polynomial complexity meaningless.

Similar problems are encountered when stating that an algorithm is of for instance cubic complexity for some range of $m$. To see this note that the function $f(m) = cm^3$ is a cubic polynomial for any finite $c$ and the previous statement does not give any hints as to what the constant $c$ may be. While the value of $c$ does not make $f(m)$ into something other than a cubic polynomial it does of course affect the values of $f(m)$ for any finite $m$.

This said, it should be stressed that complexity analysis for finite $m$ are both important and meaningful for the analysis of computer algorithms. Such analysis will provide useful insight into the behavior of the algorithms for problem sizes of practical relevance. An informative statement would in this case be that the complexity of an algorithm is well approximated by some specific function for a given range of $m$. In this instance however, the exact function would need to be given since, as previously explained, it is not sufficient to only specify it's type.

# Chapter 3

# Semidefinite Relaxation

The semidefinite relaxation (SDR) approach to detection for the linear MIMO channel was originally introduced to the area of digital communications in two seminal papers [MDW+02, TR01]. The underlying philosophy of the SDR algorithm is to, instead of solving the computationally complex ML detection problem, solve a simpler problem. The value of this is that by carefully selecting the simplified problem its solution will correspond to the true ML solution with a high degree of accuracy. Although not as widely adapted by the community as the sphere decoder of Chapter 4 the SDR algorithm has been successfully applied to various detection problems in a number of publications. As in [MDW+02, TR01] the algorithm has been further considered in the CDMA context in [ANJM02, WLA03, MDWC04]. In a few cases the algorithm has also been investigated in other contexts. In for example [SLW03] the SDR algorithm is used as an inner decoder in a system employing a concatenated coding scheme consisting of an inner space-time block-code (STBC) and an outer turbo code. In this scenario the SDR algorithm is used to obtain soft information from the inner STBC which is subsequently passed to the outer turbo decoder. Also, recently the SDR algorithm has been applied to the problem of blind decoding of orthogonal space-time block-codes [MCDX04].

A shortcoming of the semidefinite relaxation algorithm, not encountered by the sphere decoder in Chapter 4, is that it is only applicable in the case where the constellation is real valued and where $|\mathcal{S}| = 2$. The the case of a complex channel matrix with a 4-QAM constellation can however also be handled by rewriting the system on an equivalent real

valued form where the dimensions of the original problem are increased. Still, this is a restriction to the possible systems for which the semidefinite relaxation can be applied which may possibly explain why it has mainly been considered in the CDMA context.

Previously it has been shown that the SDR decoder, where it is applicable, has better performance than a class of commonly used suboptimal detectors [MDW+02]. This is accomplished by showing that the SDR represents a relaxation of the original ML detection problem and that the class of detectors under consideration represent further relaxations of the SDR. There are also analytical results which bound the performance of the SDR as compared to the exact ML solution [Nes97]. The contribution of this thesis in the area of SDR is to derive conditions under which the SDR solution corresponds to the original ML solution.

## 3.1 The Semidefinite Relaxation

Consider again the optimization problem of (2.6), i.e.

$$\hat{\mathbf{s}}_{\mathrm{ML}} = \underset{\hat{\mathbf{s}} \in \mathcal{S}^m}{\operatorname{argmin}} \|\mathbf{y} - \mathbf{H}\hat{\mathbf{s}}\|^2 \tag{3.1}$$

where now the constellation is restricted to a BPSK constellation, i.e. $\mathcal{S} = \{\pm 1\}$, and where $\mathbf{H}$ is a real valued channel matrix. Note that the case of a complex channel with a QPSK constellation, i.e. $\mathcal{S} = \{\pm 1 \pm i\}$, can also be written on this form by doubling the dimension of the original problem as

$$\begin{bmatrix} \Re(\mathbf{y}) \\ \Im(\mathbf{y}) \end{bmatrix} = \begin{bmatrix} \Re(\mathbf{H}) & -\Im(\mathbf{H}) \\ \Im(\mathbf{H}) & \Re\mathbf{H}) \end{bmatrix} \begin{bmatrix} \Re(\mathbf{s}) \\ \Im(\mathbf{s}) \end{bmatrix} + \begin{bmatrix} \Re(\mathbf{v}) \\ \Im(\mathbf{v}) \end{bmatrix}.$$

The semidefinite relaxation algorithm attempts to approximate the solution of (3.1) by forming a convex problem which has the property that the solution thereof serves as an estimate for the solution to (3.1).

To form this convex problem note that the criterion function of (3.1) can be written as

$$\|\mathbf{y} - \mathbf{H}\hat{\mathbf{s}}\|^2 = \hat{\mathbf{s}}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{H}\hat{\mathbf{s}}^{\mathrm{T}} - 2\mathbf{y}^{\mathrm{T}}\mathbf{H}\hat{\mathbf{s}} + \mathbf{y}^{\mathrm{T}}\mathbf{y}.$$

Thus $\hat{\mathbf{s}}_{\mathrm{ML}}$ can equivalently be obtained through

$$\hat{\mathbf{s}}_{\mathrm{ML}} = \underset{\hat{\mathbf{s}} \in \mathcal{S}^m}{\operatorname{argmin}} \hat{\mathbf{s}}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{H}\hat{\mathbf{s}}^{\mathrm{T}} - 2\mathbf{y}^{\mathrm{T}}\mathbf{H}\hat{\mathbf{s}}$$

since $\mathbf{y}^{\mathrm{T}}\mathbf{y}$ does not depend on $\hat{\mathbf{s}}$. The criterion function of the above problem can equivalently be written as

$$\begin{bmatrix}\mathbf{s}^{\mathrm{T}} & 1\end{bmatrix}\begin{bmatrix}\mathbf{H}^{\mathrm{T}}\mathbf{H} & -\mathbf{H}^{\mathrm{T}}\mathbf{y} \\ -\mathbf{y}^{\mathrm{T}}\mathbf{H} & 0\end{bmatrix}\begin{bmatrix}\mathbf{s} \\ 1\end{bmatrix}$$

and thus by letting $\mathbf{x} = [\hat{\mathbf{s}}^{\mathrm{T}} 1]^{\mathrm{T}}$ the ML detection problem can be solved by solving the equivalent problem

$$\begin{array}{ll}\min\limits_{\mathbf{x}\in\mathbb{R}^{m+1}} & \mathbf{x}^{\mathrm{T}}\mathbf{L}\mathbf{x} \\ \text{s.t.} & x_i^2 = 1 \quad i = 1, \ldots, m+1\end{array}$$

where $x_i$ is the $i$:th component of $\mathbf{x}$ and

$$\mathbf{L} = \begin{bmatrix}\mathbf{H}^{\mathrm{T}}\mathbf{H} & -\mathbf{H}^{\mathrm{T}}\mathbf{y} \\ -\mathbf{y}^{\mathrm{T}}\mathbf{H} & 0\end{bmatrix}.$$

It is essentially the need to write the constellation constraint on $x_i$ in the above as a quadratic form which limits the SDR approach to the case of BPSK. Note also that the constraint given by $x_{m+1} = 1$ does not need to be maintained explicitly since if a solution where $x_{m+1} = -1$ where to be obtained it is sufficient to multiply $\mathbf{x}$ by $-1$ to recover the correct solution. By introducing $\mathbf{X} = \mathbf{x}^{\mathrm{T}}\mathbf{x}$ the problem can be equivalently written as

$$\begin{array}{ll}\min\limits_{\mathbf{X},\,\mathbf{x}} & \mathrm{tr}(\mathbf{L}\mathbf{X}) \\ \text{s.t.} & \mathrm{diag}(\mathbf{X}) = \mathbf{e} \\ & \mathbf{X} = \mathbf{x}\mathbf{x}^{\mathrm{T}}\end{array} \tag{3.2}$$

where $\mathbf{e}$ is the vector of all ones. Problem (3.2) is equivalent to (3.1) in the sense that if the solution to one is known the solution to the second can be easily computed and vice verse. Still, if (3.1) is difficult to solve then so is (3.2). However, the component which make (3.2) hard is more explicit than the constraint in (3.1). To be precise, without the rank 1 constraint on $\mathbf{X}$, i.e. $\mathbf{X} = \mathbf{x}\mathbf{x}^{\mathrm{T}}$, problem (3.2) would be a convex problem.

Now, consider the convex optimization problem given by,

$$\begin{array}{ll}\min\limits_{\mathbf{X}} & \mathrm{tr}(\mathbf{L}\mathbf{X}) \\ \text{s.t.} & \mathrm{diag}(\mathbf{X}) = \mathbf{e} \\ & \mathbf{X} \succeq \mathbf{0}\end{array} \tag{3.3}$$

where $\mathbf{X} \succeq \mathbf{0}$ means that $\mathbf{X}$ is symmetric and positive semidefinite. The difference between (3.2) and (3.3) is that the constraint on $\mathbf{X}$ bas been

replaced by $\mathbf{X} \succeq 0$. Problem (3.3) is a semidefinite program and standard methods exist to solve it in polynomial time [VB96]. More specifically, by using the techniques outlined in [TR01, HRVW96, VB96] the solution can be computed with a complexity which grow as $O(m^{3.5})$. Also, if the solution, $\mathbf{X}^\star$, of (3.3) happens to be of rank 1 then it will also solve (3.2).

The rationale of studying (3.3) in the context of digital communications is that it turns out that in many cases the solution of (3.3) is indeed of rank 1 and even when this is not the case the solution to (3.2) can be correctly obtained from the solution of (3.3) with high probability. One such, in practice efficient, method for the estimation of $\hat{\mathbf{s}}_{\mathrm{ML}}$ from a high rank solution is outlined in [MDW$^+$02]. The accuracy of this method has also been analyzed previously in the literature [Nes97].

Numerical results also suggest that the proportion of rank one solutions increases with increasing SNR and decreasing condition number of the matrix $\mathbf{H}^{\mathrm{T}}\mathbf{H}$. The contribution of Section 3.2 is to provide a mathematical explanation of this behavior.

Numerical examples of the performance of the SDR algorithms, both in terms of detection accuracy as well as computational complexity, are given in Chapter 5. In that chapter the probability of obtaining a rank one solution is investigated numerically for the i.i.d. Rayleigh fading channel.

## 3.2 Rank One Analysis

As stated in the introduction it has been observed empirically that by decreasing the condition number of the channel matrix or increasing the SNR the probability of obtaining a rank 1 solution when solving (3.3) increase. The purpose of this section is to give a mathematical explanation of this behavior. Essentially, the result obtained is that the occurrence of a rank 1 solution corresponds to the event that the perturbation of $\mathbf{Hs}$ due to the noise is small. The main result of this chapter is given by Theorem 3.1 below.

**Theorem 3.1.** *Given* $\mathbf{s}$*, let the convex set* $\mathcal{V}_{\mathbf{s}}$ *be defined as*

$$\mathcal{V}_{\mathbf{s}} = \{\mathbf{v} \mid \mathbf{H}^{\mathrm{T}}\mathbf{H} + \mathbf{S}^{-1}\mathrm{Diag}(\mathbf{H}^{\mathrm{T}}\mathbf{v}) \succeq 0\} \tag{3.4}$$

*where* $\mathbf{S} = \mathrm{Diag}(\mathbf{s})$*. Then the SD relaxation (3.3) has a rank 1 solution corresponding to* $\mathbf{s}$ *if and only if* $\mathbf{v} \in \mathcal{V}_{\mathbf{s}}$*. Further, if* $\mathbf{v} \in \mathcal{V}_{\mathbf{s}}^o$*, the solution is unique.*

*Proof:* The proof is given in Appendix 3.A.1.

Note that *corresponding to* $\mathbf{s}$ is an important part of Theorem 3.1. It is possible for (3.3) to have a rank 1 solution,

$$\tilde{\mathbf{X}} = \begin{bmatrix} \tilde{\mathbf{s}} \\ 1 \end{bmatrix} \begin{bmatrix} \tilde{\mathbf{s}}^{\mathrm{T}} & 1 \end{bmatrix},$$

even when $\mathbf{v} \notin \mathcal{V}_s$ but in this case $\tilde{\mathbf{s}} \neq \mathbf{s}$.

From Theorem 3.1 it follows that for all $\mathbf{y} \in \mathcal{Y}$ where

$$\mathcal{Y} \triangleq \bigcup_{\mathbf{s} \in \mathcal{S}^m} \mathcal{Y}_{\mathbf{s}} \quad \text{and} \quad \mathcal{Y}_{\mathbf{s}} \triangleq \mathbf{H}\mathbf{s} + \mathcal{V}_{\mathbf{s}} \tag{3.5}$$

the SD relaxation is guaranteed to produce the ML estimate of $\mathbf{s}$. The sets $\mathcal{Y}_{\mathbf{s}}$ will be denoted the rank 1 regions in analogy with the ML decision regions.

The first conclusion which can be draw from Theorem 3.1 is that when the matrix $\mathbf{H}$ is of rank $m$, the product $\mathbf{H}^{\mathrm{T}}\mathbf{H}$ will be strictly positive definite and the $\mathbf{0}$ vector will lie in the interior of $\mathcal{V}_{\mathbf{s}}$. This implies that whenever $\mathbf{H}$ is of rank $m$ the probability of obtaining the ML estimate by SDR goes to 1 as the SNR increases, i.e.

$$\lim_{\sigma^2 \to 0} \mathrm{P}\left(\mathrm{Rank}(\mathbf{X}^\star) = 1\right) = 1$$

where $\mathbf{X}^\star$ is the solution of (3.3).

Further, assuming that $\mathbf{s} \in \mathcal{S}^m$ was transmitted across the channel, a necessary but not sufficient condition for $\hat{\mathbf{s}}_{\mathrm{ML}} = \mathbf{s}$ is

$$\mathbf{h}_i^{\mathrm{T}}\mathbf{h}_i + s_i^{-1}\mathbf{h}_i^{\mathrm{T}}\mathbf{v} \geq 0 \quad i \in \{1, \ldots, m\} \tag{3.6}$$

where $\mathbf{h}_i$ is the $i$:th column of $\mathbf{H}$. This condition is obtained by observing that for $\hat{\mathbf{s}}_{\mathrm{ML}} = \mathbf{s}$ the sent vector $\mathbf{s}$ should have a lower objective value in (3.1) than $\tilde{\mathbf{s}} \in \mathcal{S}^m$ where $\tilde{\mathbf{s}} = \mathbf{s} - 2s_i\mathbf{e}_i$ and $\mathbf{e}_i$ is the $i$:th unit vector, i.e. $\tilde{\mathbf{s}}$ is a vector obtained by changing the sign of one of the components of $\mathbf{s}$. If $\mathbf{H}$ has orthogonal columns then $\mathbf{H}^{\mathrm{T}}\mathbf{H}$ is diagonal and $\mathbf{v} \in \mathcal{V}_{\mathbf{s}}$ reduces to (3.6). Thus for any $\mathbf{H}$ with orthogonal columns SD relaxation always obtains the ML estimate, i.e. if $\mathbf{s}_{\mathrm{ML}} = \mathbf{s}$ then by necessity $\mathbf{v} \in \mathcal{V}_{\mathbf{s}}$. Of course, for the orthogonal channel matrix ML decoding is already a trivial problem and most suboptimal detectors are equivalent to ML for this particular case.

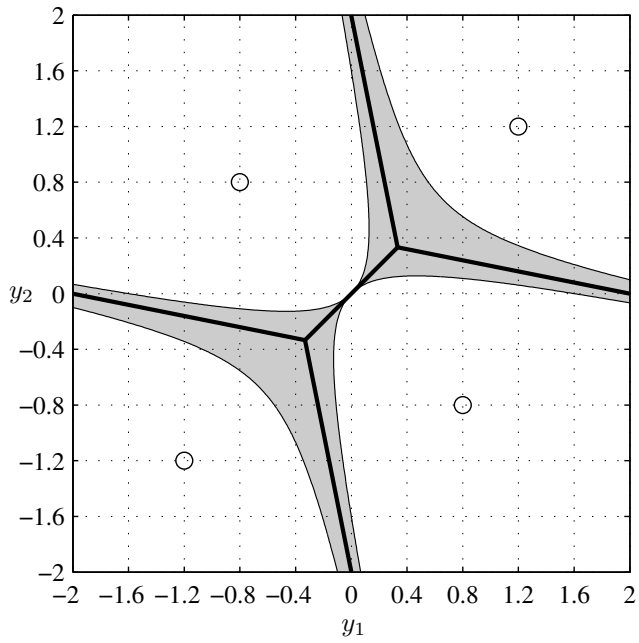


**Figure 3.1:** The rank 1 regions for a simple 2 dimensional example are shown as light regions. The noise free points, **Hs**, are shown as small circles and the boundary of the ML detection regions are shown by bold lines.

As an example, Figure 3.1 shows the rank 1 regions as a function of the received vector $\mathbf{y}$ for the case where

$$\mathbf{H} = \begin{bmatrix} 1 & 0.2 \\ 0.2 & 1 \end{bmatrix}. \tag{3.7}$$

The four white regions show $\mathcal{Y}_{\mathbf{s}}$ for all different values of $\mathbf{s} \in \mathcal{S}^2$. The boundary of the ML decision regions are shown by the bold lines. From this picture it is clear how the rank 1 regions approximate the ML detection regions. Note that $\mathcal{Y}_{\mathbf{s}}$ are subsets of the ML-detection regions which follows since the ML and SDR estimate coincides when (3.3) has a rank 1 solution. Also, note that the rank 1 regions only depend on $\mathbf{H}$ and not on the SNR.

### 3.2.1 ML Verification

A possible practical use of Theorem 3.1 is that it provides a way of establishing that a candidate estimate, $\hat{\mathbf{s}}$, is an ML solution. To this end, let $\hat{\mathbf{s}}$ be an estimate of $\mathbf{s}$ which is obtained by any detector. Let $\hat{\mathbf{v}}$ be given by

$$\hat{\mathbf{v}} \triangleq \mathbf{y} - \mathbf{H}\hat{\mathbf{s}}.$$

From Theorem 3.1 it can be seen that if $\hat{\mathbf{v}} \in \mathcal{V}_{\hat{\mathbf{s}}}$ then it is known that $\hat{\mathbf{s}} = \hat{\mathbf{s}}_{\mathrm{ML}}$. The verification of $\hat{\mathbf{v}} \in \mathcal{V}_{\hat{\mathbf{s}}}$ can be done in $O(m^3)$ time by applying a Cholesky factorization [HJ85] to the matrix of (3.4).

Using this observation enables the following reduction in average complexity of any ML detector. First estimate $\mathbf{s}$ by a simple, e.g. linear, estimator. Then test this estimate as above to see if it is the ML estimate. Then use the ML detection algorithm only in those instances when $\hat{\mathbf{v}} \neq \mathcal{V}_{\hat{\mathbf{s}}}$. The efficiency of this method is of course related to the probability that $\hat{\mathbf{v}} \in \mathcal{V}_{\hat{\mathbf{v}}}$ and this probability is strongly dependent on parameters such as the conditioning of the channel matrix and the signal to noise ratio. It is however likely that this method may be able to reduce the average complexity of the ML detection is some scenarios.

# Appendix 3.A Proofs

## 3.A.1 Proof of Theorem 3.1

*Proof:* A solution $\mathbf{X}$, satisfying $\mathbf{X} \succeq \mathbf{0}$, is an optimal solution to (3.3) if and only if there are $\mathbf{Z} \in \mathbb{R}^{m+1}$, $\mathbf{Z} \succeq \mathbf{0}$, and $\mathbf{z} \in \mathbb{R}^{n+1}$ such that [WSV00, Ch 4.2]

$$\begin{aligned} \operatorname{diag}(\mathbf{X}) &= \mathbf{e} \\ \mathbf{Z} + \operatorname{Diag}(\mathbf{z}) &= \mathbf{L} \\ \mathbf{XZ} &= \mathbf{0}. \end{aligned} \tag{3.8}$$

where $\mathbf{Z}$ and $\mathbf{z}$ are dual variables and (3.8) the Karush-Kuhn-Tucker, KKT, conditions for (3.3). Assuming that (3.3) has a rank 1 solution corresponding to $\mathbf{s}$, i.e. $\mathbf{X} = \mathbf{x}\mathbf{x}^{\mathrm{T}}$ for $\mathbf{x}^{\mathrm{T}} = [\mathbf{s}^{\mathrm{T}}\ 1]$, (3.8) implies

$$\mathbf{XZ} = \mathbf{x}\mathbf{x}^{\mathrm{T}}(\mathbf{L} - \operatorname{Diag}(\mathbf{z})) = \mathbf{0}.$$

Multiplying on the left by $\mathbf{x}^{\mathrm{T}}$ and taking the transpose yields

$$\mathbf{L}\mathbf{x} = \operatorname{Diag}(\mathbf{z})\mathbf{x}$$

and

$$\mathbf{z} = \operatorname{Diag}(\mathbf{x})^{-1}\mathbf{L}\mathbf{x}$$

where $\operatorname{Diag}(\mathbf{x})$ is invertible due to the constraint $\operatorname{diag}(\mathbf{X}) = \mathbf{e}$. The matrix $\mathbf{Z}$ is thus explicitly given by

$$\mathbf{Z} = \mathbf{L} - \operatorname{Diag}(\mathbf{x})^{-1}\operatorname{Diag}(\mathbf{L}\mathbf{x}).$$

Using the linear model given in (2.1), i.e. $\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{v}$, the matrix $\mathbf{L}$ becomes

$$\mathbf{L} = \begin{bmatrix} \mathbf{H}^{\mathrm{T}}\mathbf{H} & -\mathbf{H}^{\mathrm{T}}\mathbf{H}\mathbf{s} - \mathbf{H}^{\mathrm{T}}\mathbf{v} \\ -\mathbf{s}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{H} - \mathbf{v}^{\mathrm{T}}\mathbf{H} & 0 \end{bmatrix}$$

and using $\mathbf{x}^{\mathrm{T}} = [\mathbf{s}^{\mathrm{T}}\ 1]$, the matrix $\mathbf{Z}$ can be written as

$$\begin{aligned} &\mathbf{Z} = \mathbf{L} - \operatorname{Diag}(\mathbf{x})^{-1}\operatorname{Diag}(\mathbf{L}\mathbf{x}) = \\ &\begin{bmatrix} \mathbf{H}^{\mathrm{T}}\mathbf{H} + \mathbf{S}^{-1}\operatorname{Diag}(\mathbf{H}^{\mathrm{T}}\mathbf{v}) & -\mathbf{H}^{\mathrm{T}}\mathbf{H}\mathbf{s} - \mathbf{H}^{\mathrm{T}}\mathbf{v} \\ -\mathbf{s}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{H} - \mathbf{v}^{\mathrm{T}}\mathbf{H} & \mathbf{s}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{H}\mathbf{s} + \mathbf{s}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{v} \end{bmatrix} \end{aligned} \tag{3.9}$$

where $\mathbf{S} = \operatorname{Diag}(\mathbf{s})$. Note that $\mathbf{Z}$ can be written as

$$\begin{bmatrix} \mathbf{I} & -\mathbf{s} \end{bmatrix}^{\mathrm{T}} (\mathbf{H}^{\mathrm{T}}\mathbf{H} + \mathbf{S}^{-1}\operatorname{Diag}(\mathbf{H}^{\mathrm{T}}\mathbf{v})) \begin{bmatrix} \mathbf{I} & -\mathbf{s} \end{bmatrix}.$$

This implies that $\mathbf{Z}$ is positive semidefinite if and only if

$$\mathbf{H}^{\mathrm{T}}\mathbf{H} + \mathbf{S}^{-1}\mathrm{Diag}(\mathbf{H}^{\mathrm{T}}\mathbf{v}) \succeq 0. \tag{3.10}$$

Thus, for any $\mathbf{s} \in \mathcal{S}^m$ the optimal solution to the SDR problem will have a rank 1 solution corresponding to $\mathbf{s}$ if and only if (3.10) is positive semidefinite. This proves that $\mathbf{X} = \mathbf{x}\mathbf{x}^{\mathrm{T}}$ where $\mathbf{x} = [\mathbf{s}^{\mathrm{T}}\ 1]^{\mathrm{T}}$ is a solution to (3.3) if and only if (3.10) is satisfied. What remain to be shown is that if in addition (3.10) is satisfied with strict inequality no other $\mathbf{X}$ can solve (3.3).

To show this it is convenient to first show that there can be no solutions of rank higher than one. This can be accomplished by an indirect proof. Assume that $\mathbf{X}_1$ is a rank one solution and $\mathbf{X}_r$ is a solution of rank $r > 1$. Also note that since $r$ is arbitrary it may without loss of generality be assumed that there are no solution of rank greater than $r$. Let $\mathbf{Z}_1$ and $\mathbf{Z}_r$ be the corresponding dual optimal variables satisfying (3.8). Note also that from the above it is known that $\mathbf{Z}_1$ is uniquely given by (3.9). Further, $\mathbf{v} \in \mathcal{V}_{\mathbf{s}}^0$ implies that the matrix in (3.10) has full rank, i.e. $\mathbf{Z}_1 \in \mathbb{R}^{m+1}$ has rank $m$.

Due to the convexity of (3.3) any convex combination of $\mathbf{X}_1$ and $\mathbf{X}_r$ is also a solution. Therefore it holds that $\mathrm{Range}(\mathbf{X}_1) \subset \mathrm{Range}(\mathbf{X}_r)$ since if this were not true $\theta\mathbf{X}_1 + (1-\theta)\mathbf{X}_r$ would have rank $r+1$ for any $\theta \in (0,1)$ which would violate the assumption about $\mathbf{X}_r$ being of maximal rank. Thus, by the assumption that $r$ is the maximum rank of any solution it follows that $\mathrm{Range}(\mathbf{X}_1) \subset \mathrm{Range}(\mathbf{X}_r)$ and consequently $\mathbf{Z}_r\mathbf{X}_1 = \mathbf{0}$ since $\mathbf{Z}_r\mathbf{X}_r = \mathbf{0}$ by (3.8). This shows that the pair $(\mathbf{X}_1, \mathbf{Z}_r)$ is a valid solution of (3.8) for some $\mathbf{z}$. However, $\mathbf{Z}_r\mathbf{X}_r = \mathbf{0}$ implies that $\mathrm{Rank}(\mathbf{Z}_r) \leq m - r + 1 < m$, which proves that $\mathbf{Z}_r \neq \mathbf{Z}_1$ and contradict the uniqueness of $\mathbf{Z}_1$. Thus there can be no solutions of rank greater than 1. Also note that there can not be several solutions of rank 1 since $\mathrm{Range}(\mathbf{X}_1) \subset \mathrm{Range}(\mathbf{X}_r)$ together with $\mathrm{diag}(\mathbf{X}_r) = \mathrm{diag}(\mathbf{X}_1) = \mathbf{e}$ implies that $\mathbf{X}_r = \mathbf{X}_1$ if $r = 1$. This concludes the proof. ■

# Chapter 4

# Sphere Decoding

The underlying principles of the sphere decoder were originally developed for finding vectors of short length in lattices [Poh81, FP85]. This problem is encountered in a wide range of areas including for example problems in lattice design, Monte Carlo second-moment estimation and cryptography, see [AEVZ02]. The sphere decoder was[1] first applied to the ML detection problem in the early 90's [Mow92, VB93, Mow94] but gained main stream recognition with a later series of papers [VB99, DCB00]. The historical background as well as the current state of the art implementations of algorithm have been recently covered in two semitutorial papers [AEVZ02, DGC03].

The algorithm has found applications in most areas covered in Chapter 2. Some examples include [VH02] witch focus on the multiple antenna channel, [BB03] with focus on the CDMA scenario, and [HB03] where the sphere decoder is extended to generate soft information required by concatenated coding schemes.

To this point there has not been many papers which have treated the complexity of the algorithm analytically. The paper of Fincke and Phost [FP85] and the results covered in [HV02, HV03, AEVZ02] are noted as the exceptions. There are however a number of papers which analyze the complexity of the algorithm by simulation, e.g. [DAML01]. In both [HV02] and [DAML01] the sphere decoder is referred to as an algorithm of polynomial expected complexity. However, neither of the papers offer any stringent, i.e. analytical, proofs of the statement but still the results have been widely quoted in the literature, see e.g. [DGC03, HB03, SLW03].

[1] To the author's best knowledge.

Unfortunately however, the application of a stringent complexity analysis shows that for most scenarios encountered in digital communications, the sphere decoder is not of polynomial expected complexity but of exponential expected complexity according to the definitions of Section 2.3. One of the contributions of this chapter is the proof of this. The second contribution of this chapter is the development of an asymptotic analysis which can be applied to approximate the expected complexity of the sphere decoder for the case of the Rayleigh fading channel.

As with the SDR algorithm, the numerical examples illustrating the sphere decoder performance, both in terms of computational complexity and bit error rate, are left for Chapter 5.

## 4.1 The Sphere Decoding Algorithm

The ML detection problem of (2.6), i.e.

$$\hat{\mathbf{s}}_{\mathrm{ML}} = \underset{\hat{\mathbf{s}} \in \mathcal{S}^m}{\operatorname{argmin}} \, \|\mathbf{y} - \mathbf{H}\hat{\mathbf{s}}\|^2$$

can alternatively be written as

$$\hat{\mathbf{s}}_{\mathrm{ML}} = \underset{\hat{\mathbf{s}} \in \mathcal{S}^m}{\operatorname{argmin}} \, \|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|^2 \tag{4.1}$$

where $\mathbf{QR} = \mathbf{H}$ for $\mathbf{Q} \in \mathbb{C}^{m \times n}$, $\mathbf{R} \in \mathbb{C}^{m \times m}$ is the QR decomposition [HJ85] of $\mathbf{H}$, i.e. $\mathbf{Q}$ is a matrix with orthonormal columns and $\mathbf{R}$ is upper triangular, and where $\mathbf{x} = \mathbf{Q}^{\mathrm{H}}\mathbf{y}$. The idea behind the sphere decoder is to solve (4.1) by enumerating all points which belong to a hypersphere of radius $r$ around the received point $\mathbf{x}$. That is, all $\hat{\mathbf{s}} \in \mathcal{S}^m$ which satisfy a criterion on the form given by

$$\|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|^2 \leq r^2 \tag{4.2}$$

and where the issue of choosing a suitable $r$ will be discussed at length later. Clearly nothing would be gained if the condition of (4.2) had to be verified for all $\hat{\mathbf{s}} \in \mathcal{S}^m$. However, the algorithm originally proposed in [Poh81, FP85] provides an efficient enumeration strategy for the points which do belong to the sphere. This enumeration is based on the following observation. Let

$$\mathbf{p} \triangleq \mathbf{x} - \mathbf{R}\hat{\mathbf{s}}$$

and let $\mathbf{p}_{\iota_k} \in \mathbb{C}^k$ be the vector composed of the $k$ last components of $\mathbf{p}$. Then

$$\|\mathbf{p}_{\iota_k}\|^2 > r^2 \quad \Rightarrow \quad \|\mathbf{p}\|^2 > r^2.$$

Further, due to the upper triangular structure of $\mathbf{R}$ the vector $\|\mathbf{p}_{\iota_k}\|$ depends only on $\hat{\mathbf{s}}_{\iota_k}$ where $\hat{\mathbf{s}}_{\iota_k} \in \mathcal{S}^k$ is the vector composed of the last $k$ components of $\hat{\mathbf{s}}$. Therefore, by establishing that $\|\mathbf{p}_{\iota_k}\|^2 > r^2$ for some vector $\hat{\mathbf{s}} \in \mathcal{S}^m$ and index $k$, any other vector $\tilde{\mathbf{s}} \in \mathcal{S}^m$ for which $\tilde{\mathbf{s}}_{\iota_k} = \hat{\mathbf{s}}_{\iota_k}$ may be excluded from the search.

The sphere decoder uses this observation in a structured manner to efficiently enumerate all points in the hypersphere given by (4.2). Let $\mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ be the set of points $\bar{\mathbf{s}} \in \mathcal{S}^k$ for which $\bar{\mathbf{s}}_{\iota_{k-1}} = \bar{\mathbf{s}}_{k-1}$, i.e.

$$\mathcal{P}_k(\bar{\mathbf{s}}_{k-1}) \triangleq \{\bar{\mathbf{s}} \in \mathcal{S}^k \mid \bar{\mathbf{s}}_{\iota_{k-1}} = \bar{\mathbf{s}}_{k-1}\}$$

and let the otherwise ill defined $\mathcal{P}_1(\bar{\mathbf{s}}_0)$ be

$$\mathcal{P}_1(\bar{\mathbf{s}}_0) \triangleq \mathcal{S}$$

for notational convenience. That is, $\mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ is the set of possible symbol vectors in $\mathcal{S}^k$ which can be constructed by adding one symbol to $\bar{\mathbf{s}}_{k-1}$. Further, let $\mathcal{R}_k$ be the set of points in $\mathcal{S}^k$ which are not violating the sphere constraint of (4.2), i.e.

$$\mathcal{R}_k \triangleq \{\bar{\mathbf{s}} \in \mathcal{S}^k \mid \|\mathbf{x}_{\iota_k} - \mathbf{R}_{\iota_k}\bar{\mathbf{s}}\|^2 \leq r^2\} \tag{4.3}$$

where $\mathbf{R}_{\iota_k} \in \mathbb{C}^{k\times k}$ is the $k \times k$ lower right block of $\mathbf{R}$. The enumeration procedure can be described by the following algorithm which enumerates all points satisfying (4.2) recursively, starting with $k = 1$.

Algorithm: ENUM($k$,$\bar{\mathbf{s}}_{k-1}$)

1: **for** $\bar{\mathbf{s}}_k \in \mathcal{R}_k \cap \mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ **do**
2: **if** $k = m$ **then**
3: save $\hat{\mathbf{s}} = \bar{\mathbf{s}}_k$
4: **else**
5: ENUM($k + 1$,$\bar{\mathbf{s}}_k$)
6: **end if**
7: **end for**

In the above, note that $\bar{\mathbf{s}}_k$ is the vector given by $\bar{\mathbf{s}}_k = [\bar{s}_{m-k+1} \dots \bar{s}_m]^{\mathrm{T}}$. The algorithm can be interpreted as a tree pruning algorithm, see Figure 4.1. The algorithm visits the nodes in the tree from top to bottom. At each depth, $k$, it is verified if some choice of $\bar{s}_{m-k+1} \in \mathcal{S}$ will satisfy $[\bar{s}_{m-k+1}\ \bar{\mathbf{s}}_{k-1}^{\mathrm{T}}]^{\mathrm{T}} \in \mathcal{R}_k$ where $\bar{\mathbf{s}}_{k-1}$ is the previous choice made for the symbols $\bar{s}_i$ where $i = m - k + 2, \dots, m$. This is equivalent to verifying if $\mathcal{R}_k \cap \mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ is empty or not. If there are any possible values for

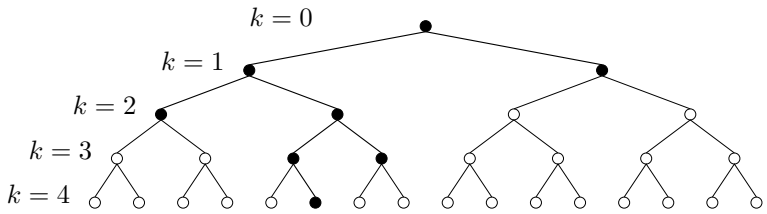


**Figure 4.1:** The ML problem illustrated as s search tree for a problem of size $m = 4$ and symbol set of cardinality $|\mathcal{S}| = 2$. Nodes visited by the sphere decoder are shown in black.

$\bar{s}_{m-k+1}$ the algorithms proceeds further down the tree by the branches given by $\bar{s}_{m-k+1}$. If not, the algorithm goes up in the tree, updates previous choices of $\bar{s}_i$ and proceeds down another branch. Whenever the algorithm reaches depth $k = m$ all points in $\mathcal{R}_k \cap \mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ satisfy (4.2) and are saved before the algorithms continues.

At the end of the enumeration stage the saved symbol vector, assuming such vectors exist, which yields the smallest value of the criterion function in (4.1) will correspond to the ML estimate and is therefore chosen as the output of the algorithm.

### Further Improvements

An common improvement [DGC03] over the algorithm described so far is to at Line 3 of ENUM update the parameter $r$ such that

$$\|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|^2 = r^2$$

for the $\hat{\mathbf{s}}$ currently being enumerated. This ensures that after obtaining an $\hat{\mathbf{s}}$ in the sphere the radius is decreased so that no other points which is further away from $\mathbf{x}$ than $\mathbf{R}\hat{\mathbf{s}}$ are enumerated. The benefit of this improvement is strongly dependent on the specific order in which the points $\bar{\mathbf{s}}_k \in \mathcal{R}_k \cap \mathcal{P}_k(\bar{\mathbf{s}}_{k-1})$ on Line 1 of ENUM are enumerated. The reason for this is that by proper ordering, the radius, $r$, may be decreased early on in the enumeration which keeps many nodes in the tree of Figure 4.1 from being visited at all. The currently most popular ordering strategy is referred to as the Schnorr-Euchnerr strategy [SE94, AEVZ02]. This strategy enumerate the points based on their distance to a linear estimate of $\hat{s}_k$ based on $\hat{s}_i$ for $i = m - k + 2, \ldots, m$.

Another improvement over the original algorithm is obtained by permuting the columns of the channel matrix $\mathbf{H}$ prior to decoding. By permuting the columns of $\mathbf{H}$, which changes the order in which the components of $\hat{\mathbf{s}}$ are investigated, the $\mathbf{R}$ matrix is also changed. Here it is less clear which strategy is to be preferred. However, a few of the commonly used strategies are covered in [DGC03], see also [WMPF03]. However, in this chapter such permutation strategies will not be further considered.

A subtle but important point which has not yet been addressed is how the radius, $r$, is to be chosen. It is clear that if the sphere decoder are to solve the ML detection problem the parameter $r$ must be at least as large as $r^\star$ where $r^\star$ is given by

$$r^\star \triangleq \min_{\hat{\mathbf{s}} \in \mathcal{S}^m} \|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|.$$

However, in order to choose $r$ based on this criterion would require the solution of the problem in advance. There are several computationally efficient strategies for choosing $r$ proposed in the literature [HV02, DCB00, BB03]. One of the better strategies is given in [HV02] where the radius is chosen based on the statistics of $\|\mathbf{x} - \mathbf{R}\mathbf{s}\|^2$ where $\mathbf{s}$ is the transmitted vector. The issue of choosing the radius, or the initial radius in the case where it is adaptively updated, will be further discussed in Section 4.2.1.

## 4.2 Complexity Analysis

The complexity of the sphere decoder will be proportional to the number of nodes visited in the search tree, i.e. the number of black nodes in Figure 4.1 or the number of times Line 2 in the ENUM algorithm is executed. Since the number of numerical operations required for each pass of Line 2 is at most polynomial in $k$ [FP85] the sphere decoder will be of polynomial complexity if the number of nodes visited grows polynomially in $m$ and of exponential complexity if the number of visited nodes grows exponentially.

Let $N$ be the number of nodes visited by the sphere decoder for a given $\mathbf{H}$ and $\mathbf{y}$, i.e.

$$N(\mathbf{H}, \mathbf{y}) = N \triangleq 1 + \sum_{k=1}^{m} |\mathcal{R}_k|$$

where $\mathcal{R}_k$ is defined in (4.3) and the additional 1 is for the top level node. Let the expected complexity, $C = C(m)$, be the expected value of

$N$ where the expectation is computed over the distributions of $\mathbf{H}$ and $\mathbf{y}$ induced by the assumption on $\mathbf{H}$ and the model given in (2.1), i.e.

$$C \triangleq \mathrm{E}_{\mathbf{H},\mathbf{y}} \left\{ N(\mathbf{H}, \mathbf{y}) \right\}. \tag{4.4}$$

Previously, there have been claims that $C(m)$ under some conditions grows polynomially [HV02, DAML01] in $m$. As the detection problem itself is NP-hard it would be, although theoretically possible, a truly remarkable result if the expected complexity was polynomial for the channel models commonly encountered in digital communications. This is however unfortunately not the case. The problem with the analysis of for instance [HV02] is that $m$ is restricted to some bounded interval. By doing so the definition of polynomial complexity given in Section 2.3 is no longer applicable and it is therefore unclear what the authors actually mean by polynomial complexity. This issue was further elaborated on in Section 2.3.2. In another case where polynomial complexity is analytically shown [FP85] a key assumption is that $r$ is fixed and independent of $m$. However, in the following section it will be argued that this assumption is not realistic for the ML detection problem considered herein and therefore the results of [FP85] are not directly applicable to the digital communications scenario.

A key result of this work is that under some assumptions, applicable to a large class of communications systems, $C(m)$ is in fact exponential in $m$. This is shown in Section 4.2.2. Then, in Section 4.3, the exact exponent is computed for the i.i.d. Rayleigh fading channel.

### 4.2.1 The Sphere Radius

As is indicated above the choice of sphere radius, $r$, will have an impact on the performance of the sphere decoder. If the radius, $r$, is chosen too small, no points will lie inside the search sphere and the algorithm will fail. This is clearly unacceptable, at least if this occurs with high probability. At the same time, if the radius is chosen to large the algorithm will be forced to search over many points and be inefficient.

In order to analyze the complexity of the sphere decoder some assumptions about the radius must however inevitably be made. It is of course desirable to have assumptions which include as many of the proposed versions of the sphere decoder as possible. However, explicit assumptions about the choice of $r$ are bound to complicate the analysis of the algorithm. It can however be argued that for any reasonable implementations of the sphere decoder the squared radius must essentially grow as a linear

function of the problem size. To see this note that, due to the observations made in [HV02], the probability that the transmitted message, $\mathbf{s}$, belongs to a sphere of squared radius $r^2 = \kappa\sigma^2 m$ may be computed as

$$\mathrm{P}\left(\|\mathbf{x} - \mathbf{R}\mathbf{s}\|^2 \leq \kappa\sigma^2 m\right) = \mathrm{P}\left(\|\mathbf{Q}^{\mathrm{H}}\mathbf{v}\|^2 \leq \kappa\sigma^2 m\right).$$

Since, by the law of large numbers,

$$\lim_{m\to\infty} \frac{1}{m}\|\mathbf{Q}^{\mathrm{H}}\mathbf{v}\|^2 = \sigma^2 \quad \text{a.s.}$$

this probability will tend to 1 for any $\kappa > 1$. This shows that the squared radius, $r^2 = r_m^2$, is not required to grow faster than a linear function in $m$ in order to maintain high probability of solving the ML detection problem.

Similarly, it is possible to show that the radius $r_m^2$ also must grow at least as fast as a linear function in $m$ for the probability of failure to remain low. However, to as above assume that $r_m$ is based on the statistics of the noise alone, will not capture many of the more advanced implementations of the sphere decoder. In general $r_m$ may be chosen as some function of the input parameters. It is still however possible to show that for any reasonable choice of such a function, $r_m^2$ must essentially grow as a linear function of $m$. This is formalized by the following theorem.

**Theorem 4.1.** *Assume that the radius $r = r_m$ is chosen as some function of the input parameters, i.e.*

$$r_m : \mathbb{C}^{n\times m} \times \mathbb{C}^n \mapsto \mathbb{R}$$

*were $r = r_m(\mathbf{H}, \mathbf{y})$. Let $\mathcal{D}_m$ be the event that the sphere decoder obtains the ML solution, i.e. that the search sphere is not empty. Then*

$$\liminf_{m\to\infty} \mathrm{P}\left(\mathcal{D}_m\right) \geq \nu$$

*imply*

$$\liminf_{m\to\infty} \mathrm{P}\left(r_m^2 \geq \kappa\sigma^2 m\right) \geq \nu$$

*for any $\kappa \in (0, |\mathcal{S}|^{-1})$.*

*Proof:* The proof is given in Appendix 4.A.1.

Thus, by Theorem 4.1 any strategy of choosing $r_m$ which does not have a vanishing probability of solving the ML detection problem will also have a non-vanishing probability that $r_m^2$ is larger than a linear function in $m$.

### 4.2.2 Proving Exponential Expected Complexity

In order to study the complexity of the sphere decoder it is convenient to introduce the notion of search depth. Therefore, let the *search depth*, $d(\hat{\mathbf{s}})$, be the depth at which a particular path, $\hat{\mathbf{s}}$, in the search tree is cut of, i.e.

$$d(\hat{\mathbf{s}}) \triangleq \sup\left(0 \cup \{k \in \mathbb{N} \mid 1 \leq k \leq m,\ \hat{\mathbf{s}}_{\iota_k} \in \mathcal{R}_k\}\right). \tag{4.5}$$

where $\mathcal{R}_k$ is given by (4.3). For a given $\mathbf{H}$ and $\mathbf{y}$ the search dept is a function of $\hat{\mathbf{s}}$. However, by assigning a probability distribution to $\hat{\mathbf{s}}$ the search depth, $d = d(\hat{\mathbf{s}})$, may be viewed as a random variable with a probability distribution induced by the distributions of $\mathbf{H}$, $\mathbf{y}$ and $\hat{\mathbf{s}}$. Any analysis of the complexity of sphere decoding will inevitably involve counting the number of nodes visited in the search tree. However, by assigning a uniform input distribution to $\hat{\mathbf{s}}$ the number of nodes in the search tree may be expressed in terms of the statistics of $d$. The value of such a reformulation will become apparent later on as tools from probability theory are used to address questions about the complexity of the algorithm. The following lemma, which all subsequent complexity analysis will be based on, forms the basis of this probabilistic approach to the complexity analysis.

**Lemma 4.2.** *Let $d = d(\hat{\mathbf{s}})$ be the stochastic variable defined by (4.5) with a probability distribution induced by $\mathbf{H}$, $\mathbf{y}$ and $\hat{\mathbf{s}}$ when $\hat{\mathbf{s}}$ is uniformly distributed over the set $\mathcal{S}^m$. Then*

$$C = \frac{\mathrm{E}\left\{|\mathcal{S}|^{d+1}\right\} - 1}{|\mathcal{S}| - 1},$$

*where $C$ is the expected number of nodes visited by the sphere decoder.*

*Proof:* The proof is given in Appendix 4.A.2.

An immediate consequence of Lemma 4.2 is that, by Jensen's inequality [Dur96] and since $|\mathcal{S}|^d$ is a convex function in $d$, a lower bound on the complexity is given by

$$C(m) \geq \frac{|\mathcal{S}|^{\mathrm{E}\{d\}+1} - 1}{|\mathcal{S}| - 1}.$$

This implies that the expected complexity of the sphere decoder will be exponential whenever $\mathrm{E}\{d\}$ grows linearly in $m$. The theorem below establishes sufficient conditions for this to apply.

**Theorem 4.3.** *Assume there is some finite $\rho_s$ such that*

$$\frac{\mathrm{E}\left\{\|\mathbf{h}_i s_i\|^2\right\}}{\sigma^2} \leq \rho_s \tag{4.6}$$

*where $\mathbf{h}_i$ is the i:th column of $\mathbf{H}$ and let for an arbitrary $\kappa > 0$ the probability, $\nu > 0$, be given by*

$$\nu \triangleq \mathrm{P}\left(r^2 \geq \kappa\sigma^2 m\right)$$

*Then the expected complexity may be lower bounded as*

$$C(m) \geq \frac{\nu|\mathcal{S}|^{\eta m} - 1}{|\mathcal{S}| - 1} \quad \textit{where} \quad \eta = \frac{\nu\kappa}{4\rho_s + 2}.$$

*Proof:* The proof is given in Appendix 4.A.3.

The assumption of (4.6) is included to ensure that the signal to noise ratio experienced by any particular symbol, $s_i$, is not allowed to tend to infinity when the size of the problem is increased. Therefore, under this assumption, by combining Theorem 4.1 and Theorem 4.3 it follows that

$$\liminf_{m\to\infty} \mathrm{P}\left(\mathcal{D}_m\right) \geq \nu > 0 \quad \Rightarrow \quad \liminf_{m\to\infty} \frac{1}{m} \ln C(m) \geq \frac{\nu \ln|S|}{(4\rho_s + 2)|\mathcal{S}|} > 0.$$

Thus, for any sequence of channel matrices satisfying (4.6) the sphere decoder is of exponential complexity given that the probability of solving the ML detection problem does not tend to zero as $m$ is increased. Note that since no explicit assumptions are made about $r_m(\mathbf{H}, \mathbf{y})$ this statement holds even in the case where the radius is adaptively updated during the search. To see this, note that if the radius where updated during the search for some sphere decoder, A, then there is another version, B, without an adaptive radius but with the minimum radius obtained by A as its initial radius. Note that the complexity of A is lower bounded by the complexity of B and that the complexity of B is exponential by the above.

On a final note it should again be emphasized that in this analysis permutations of the columns of $\mathbf{H}$ and symbol vector $\hat{\mathbf{s}}$ is not considered. While it is not likely that such an improvement of the sphere decoder will yield a version of the algorithm with polynomial expected complexity this is strictly speaking still an open problem. Note however that in the chase where permutation of $\mathbf{H}$ is such that the permuted channel matrix satisfies the assumptions made in this section the results follows

by just changing the definition of $\mathbf{H}$. The technical point which cause the proofs presented herein to fail is that most permutation strategies used in practise tend to increase the norm of some columns of the channel matrix and may induce a statistical dependence between $\mathbf{H}$ and $\mathbf{s}$.

## 4.3 Asymptotic Analysis

By the result in the previous section it is clear that the expected complexity of the sphere decoder is exponential in $m$. The bound used to prove this is however extremely loose. This is in part due to simplifications made in the derivation but also due to the generous assumptions about the statistics of $\mathbf{H}$. Thus, by making stronger assumptions about both $\mathbf{H}$ and the radius, $r$, much sharper results may be obtained.

In this section an asymptotic analysis of $C(m)$ is carried out by restricting attention to a special class of channel matrices $\mathbf{H}$. Specifically, attention is restricted to the class of i.i.d. Rayleigh fading MIMO channels where the elements of $\mathbf{H} \in \mathbb{C}^{m\times m}$ are i.i.d. zero-mean normally distributed with variance $m^{-1}$. It will further be assumed that $\mathrm{E}\left\{|s_i|^2\right\} = 1$. The normalization of $\mathbf{H}$ and $\mathbf{s}$ ensures that the SNR, $\rho$, is independent of the size, $m$, that is

$$\rho = \frac{\mathrm{E}\left\{\|\mathbf{Hs}\|^2\right\}}{\mathrm{E}\left\{\|\mathbf{v}\|^2\right\}} = \sigma^{-2}.$$

Note that the choice of scaling $\mathbf{H}$, $\mathbf{s}$ or $\mathbf{v}$ in order to fix the SNR is completely arbitrary and does not affect the conclusions made in this section.

The particular class of channel matrices studied in the section has previously been studied in [HV02][2] where an exact expression for the expected complexity was also derived for the case when the radius is chosen as $r^2 = \kappa\sigma^2 m$ for some $\kappa > 0$. The complexity expression of [HV02] is however somewhat complicated and becomes increasingly cumbersome to compute for larger $m$. Therefore, the value of an asymptotic analysis lies in the analytical simplicity of the results which may be obtained. It will be the goal of this section to compute the exponent of the complexity, $C(m)$, i.e. to obtain results on the following form.

$$C(m) \doteq e^{\gamma m} \tag{4.7}$$

[2]Only real valued matrixes where considered in [HV02] but the analysis is readily extended to the complex case.

where $\doteq$ means *equal to the first order in the exponent* and is equivalent to the statement

$$\lim_{m\to\infty} \frac{1}{m} \ln C(m) = \gamma \tag{4.8}$$

for some $\gamma \in \mathbb{R}$. The intuitive interpretation of this notation is that $C(m)$ behaves roughly as the exponential function on the right hand side of (4.7) for large $m$.

As stated before the complexity of the algorithm, and therefore $\gamma$, is dependent on the way which the radius, $r = r_m$, of the sphere is chosen. Therefore, to enable the analysis of the asymptotic complexity and motivated by Section 4.2.1 the radius is assumed to satisfy

$$\lim_{m\to\infty} \frac{r_m^2}{m} = \kappa\sigma^2 \tag{4.9}$$

for some fixed $\kappa > 0$. It is also assume that $r_m$ is statistically independent of $\mathbf{H}$ and $\mathbf{y}$. Note that the important special case when $r_m$ is chosen such that

$$\mathrm{P}\left(\|\mathbf{y} - \mathbf{H}\mathbf{s}\| \leq r_m^2\right) = 1 - \epsilon_m$$

for any sequence $\{\epsilon_m\}_{m=1}^{\infty}$ where

$$\liminf_{m\to\infty} \epsilon_m > 0 \quad \text{and} \quad \limsup_{m\to\infty} \epsilon_m < 1$$

satisfies these assumptions with $\kappa = 1$. Although not obvious at this point, the assumption about $r_m$ in (4.9) together with the i.i.d. Gaussian distribution of $\mathbf{H}$ are sufficient for the existence of the limit in (4.8) for any constellation, $\mathcal{S}$, and SNR, $\rho > 0$. This will be shown in the following section.

### 4.3.1 Computing the Asymptotic Rate

In order to establish the existence of, and to compute, the limit in (4.8) it is convenient to again consider the search depth, $d$, of (4.5) and to define

$$z_m \triangleq \frac{d}{m}$$

as the *normalized search depth*. Due to the normalization $\{z_m\}_{m=1}^{\infty}$ is a sequence of random variables taking values in $[0, 1]$. The statistics of $z_m$ are those induced by $\mathbf{H}$, $\mathbf{s}$, $\hat{\mathbf{s}}$, $\mathbf{v}$ and by the choice of $r_m$. First, note that from Lemma 4.2 it can be seen that

$$\lim_{n\to\infty} \frac{1}{m} \ln C(m) = \lim_{n\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \tag{4.10}$$

whenever the limit on the right hand side exists since only the term $\mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\}$ will affect the asymptotic behavior of $C(m)$. Therefore, attention may be restricted to this expected value. The rationale behind introducing the normalized search depth is that it can be shown that the limit

$$\lim_{n\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\}$$

can be computed from the probability that $z_m$ is larger than some fraction of the range $[0, 1]$. This is formalized by Theorem 4.4 below. Note that this result is closely related to a more general theorem from large deviations theory which is referred to as Varadhan's integral Lemma [DZ98]. The proof given herein follows the proof of Varadhand's integral Lemma given in [SW95]. However, a reason for presenting the proof in full is that in this particular case the proof itself is simpler than proving the assumptions[3] needed for the general theorem.

**Theorem 4.4.** *Let $g(a)$ be given by*

$$g(a) \triangleq -\lim_{m\to\infty} \frac{1}{m} \ln \mathrm{P}\left(z_m \geq a\right).$$

*If the limit exists for all $a \in [0, 1]$, then*

$$\mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \doteq e^{\gamma m}$$

*where*

$$\gamma = \sup_{0\leq a\leq 1} \left(a \ln |\mathcal{S}| - g(a)\right).$$

*Proof:* The proof is given in Appendix 4.A.4.

To interpret Theorem 4.4 note that the expected value of (4.10) is lower bounded as

$$\mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \geq |\mathcal{S}|^{ma} \mathrm{P}\left(z_m \geq a\right) \doteq e^{(a \ln |\mathcal{S}| - g(a))m}$$

for any $a \in [0, 1]$. What Theorem 4.4 states is that the best bound of this type, which is obtained by maximizing over the free parameter $a$, is tight in the sense that it gives the correct linear term in the exponent.

[3] The use of Varadhan's integral Lemma in it's standard form would require proving that $\{z_m\}_{m=1}^{\infty}$ satisfies a large deviation principle [DZ98]. In this case however, particulary since $|\mathcal{S}|^{mz_m}$ is increasing in $z_m$, this is not required for the conlusion to hold.

However, to compute $g(a)$ from $z_m$ directly is difficult due to the explicit dependence of $z_m$ on the radius $r_m$ among other things. Therefore it is convenient to first introduce bounds on $\mathrm{P}(z_m \geq a)$ which are analytically simpler but still capture the asymptotic nature of $z_m$. Such bounds are given by the following theorem.

**Theorem 4.5.** *Let the sequence of stochastic variables $\{w_k\}_{k=1}^{\infty}$ be given by*

$$w_k \triangleq \frac{1}{k}\sum_{i=1}^{k} |q_i|^2$$

*where $\{q_i\}_{i=1}^{\infty}$ are i.i.d. $\mathcal{N}_C(0,1)$. Similarly, let $\{u_k\}_{k=1}^{\infty}$ be given by*

$$u_k \triangleq \frac{1}{k}\sum_{i=1}^{k} \frac{|s_i - \hat{s}_i|^2}{2}$$

*where $\{s_i\}_{i=1}^{\infty}$ and $\{\hat{s}_i\}_{i=1}^{\infty}$ are i.i.d. $\mathcal{U}(\mathcal{S})$. Let $P(\alpha, k)$ be given by*

$$P(\alpha, k) \triangleq \mathrm{P}\left(\left(2\rho\alpha^2 u_k + \alpha\right) w_k \leq \kappa\right). \tag{4.11}$$

*Then, for any $\alpha > a$ there is an $M$ such that*

$$\mathrm{P}(z_m \geq a) \geq P(\alpha, \lceil am \rceil) \tag{4.12}$$

*for $m \geq M$ and for any $\alpha < a$ there is an $M$ such that*

$$\mathrm{P}(z_m \geq a) \leq P(\alpha, \lceil am \rceil) \tag{4.13}$$

*for $m \geq M$.*

*Proof:* The proof is given in Appendix 4.A.5.

While not obvious at this stage the function $P(\alpha, k)$ will also have the appealing properly that

$$P(a, \lceil am \rceil) \doteq \mathrm{P}(z_m \geq a). \tag{4.14}$$

Thus, the asymptotic behaviour of $\mathrm{P}(z_m \geq a)$ may be obtained from the analysis of $P(a, \lceil am \rceil)$. In order to compute the exponential rate of $P(a, \lceil am \rceil)$ note that

$$\lim_{m\to\infty} \frac{1}{m} \ln P(a, \lceil am \rceil) = \lim_{k\to\infty} \frac{a}{k} \ln P(a, k) = a \lim_{k\to\infty} \frac{1}{k} \ln P(a, k)$$

which follows by letting $k = \lceil am \rceil$ and by noting that

$$\lim_{m\to\infty} \frac{\lceil am \rceil}{m} = a.$$

Thus

$$\lim_{m\to\infty} \frac{1}{m} \ln P(a, \lceil am \rceil)$$

may be obtained from the limit

$$\lim_{k\to\infty} \frac{1}{k} \ln P(a, k).$$

To compute this limit it is convenient to write $P(\alpha, k)$, originally given in (4.11), as

$$P(\alpha, k) = \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right) \tag{4.15}$$

where

$$\mathcal{A}_\alpha \triangleq \{(u, w) \mid (2\rho\alpha^2 u + \alpha)w \leq \kappa\}. \tag{4.16}$$

Now, the limit

$$\lim_{k\to\infty} \frac{1}{k} \ln P(a, k) = \lim_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right)$$

is written on a form which may be computed using the following theorem.

**Theorem 4.6 (Cramér's theorem for vectors in $\mathbb{R}^d$).** *Let $\{\boldsymbol{\zeta}_i\}_{i=1}^{\infty}$ be i.i.d. stochstic vectors in $\mathbb{R}^d$. Let*

$$\boldsymbol{\xi}_k = \frac{1}{k} \sum_{i=1}^{k} \boldsymbol{\zeta}_i$$

*be the empirical mean of $\boldsymbol{\zeta}_i$. Define the logarithmic moment generating function, $\Lambda(\boldsymbol{\lambda})$ for $\boldsymbol{\lambda} \in \mathbb{R}^d$, as*

$$\Lambda(\boldsymbol{\lambda}) \triangleq \ln \mathrm{E}\left\{e^{\boldsymbol{\lambda}^{\mathrm{T}} \boldsymbol{\xi}_1}\right\}.$$

*Also, let the rate function $I(\boldsymbol{\xi})$ be given by*

$$I(\boldsymbol{\xi}) = \sup_{\boldsymbol{\lambda}\in\mathbb{R}^d} \left(\boldsymbol{\lambda}^{\mathrm{T}} \boldsymbol{\xi} - \Lambda(\boldsymbol{\lambda})\right).$$

*Then, if $\Lambda(\boldsymbol{\lambda}) < \infty$ for $\boldsymbol{\lambda}$ in some neighborhood of $\mathbf{0}$, it holds that*

$$\limsup_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left(\boldsymbol{\xi}_k \in \mathcal{F}\right) \leq - \inf_{\boldsymbol{\xi}\in\mathcal{F}} I(\boldsymbol{\xi})$$

*for any closed set* $\mathcal{F} \subset \mathbb{R}^d$ *and*

$$\liminf_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left(\boldsymbol{\xi}_k \in \mathcal{G}\right) \geq - \inf_{\boldsymbol{\xi}\in\mathcal{G}} I(\boldsymbol{\xi})$$

*for any open set* $\mathcal{G} \subset \mathbb{R}^d$.

*Proof:* The proof is given in [DZ98].

Theorem 4.6 is particularly useful for sets, $\mathcal{A}$, which have the property[4] that

$$\inf_{\boldsymbol{\xi}\in\mathcal{A}^o} I(\boldsymbol{\xi}) = \inf_{\boldsymbol{\xi}\in\bar{\mathcal{A}}} I(\boldsymbol{\xi}). \tag{4.17}$$

This is because for such as set the upper and lower bounds of Theorem 4.6 imply that

$$\lim_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left(\boldsymbol{\xi}_k \in \mathcal{A}\right) = - \inf_{\boldsymbol{\xi}\in\mathcal{A}} I(\boldsymbol{\xi}).$$

As it turns out the sets of interest, $\mathcal{A}_\alpha$, have this property for any $\alpha \in [0,1]$ and

$$\lim_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right) \tag{4.18}$$

may be computed as

$$\lim_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right) = \inf_{(u,w)\in\mathcal{A}_\alpha} I(u,w)$$

where $I(u,w)$ is the rate function for $(u_k, w_k)$. Therefore, by computing the rate function for $(u_k, w_k)$ the limit of (4.18) may be obtained.

In order to compute $I(u,w)$ let $\boldsymbol{\lambda} = [\lambda_1 \ \lambda_2]^{\mathrm{T}}$ and note that

$$\ln \mathrm{E}\left\{e^{\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{\xi}_1}\right\} = \ln \mathrm{E}\left\{e^{u_1\lambda_1 + w_1\lambda_2}\right\} = \ln \mathrm{E}\left\{e^{u_1\lambda_1}\right\} + \ln \mathrm{E}\left\{e^{w_1\lambda_2}\right\}$$

due to the independence of $u_1$ and $w_1$. The rate function $I(u,w)$ may thus be obtained as

$$I(u,w) = I_u(u) + I_w(w)$$

where

$$I_u(u) \triangleq \sup_{\lambda} \left[u\lambda - \ln \mathrm{E}\left\{e^{\lambda u_1}\right\}\right] \tag{4.19}$$

[4] A set, $\mathcal{A}$, with this property is referred to as an I-continuity set [DZ98]. Also, note that this property is dependent on the rate function as well as the set.

and

$$I_w(w) \triangleq \sup_{\lambda} \left[ w\lambda - \ln \mathrm{E}\left\{ e^{\lambda w_1} \right\} \right]. \tag{4.20}$$

The former, $I_u(u)$, is dependent on the input alphabet, $\mathcal{S}$, and in general there is no closed form expression for $I_u(u)$. The later, $I_w(w)$, may however be explicitly computed. To do so, let $w_1 = q_R^2 + q_I^2$ where $q_R$ and $q_I$ are the real and imaginary parts of $q_1$ respectively, then

$$\mathrm{E}\left\{ e^{\lambda w_1} \right\} = \int_{\mathbb{R}^2} e^{\lambda(q_R^2+q_I^2)} \frac{1}{\pi} e^{-(q_R^2+q_I^2)} dq_R dq_I = \frac{1}{1-\lambda}$$

for $\lambda < 1$ and $\infty$ otherwise. Thus, $I_w(w)$ can be computed as

$$I_w(w) = \sup_{\lambda} \left[ w\lambda + \ln(1-\lambda) \right] = w - 1 - \ln w.$$

While lacking a closed form expression, the function $I_u(u)$ can always be evaluated numerically by computing

$$\mathrm{E}\left\{ e^{\lambda u_1} \right\} = \frac{1}{|\mathcal{S}|^2} \sum_{s \in \mathcal{S}} \sum_{\hat{s} \in \mathcal{S}} e^{\frac{\lambda}{2}|s-\hat{s}|^2}$$

and numerically maximizing (4.19). The only caveat is that the number of terms in the sum is equal to $|\mathcal{S}|^2$ which may make the computation cumbersome for large constellations. However, it can always be done in theory. Also, in many situations the constellation inhibits special structure which may be used to lower the complexity of the computation.

By using the rate functions $I_u(u)$ and $I_w(w)$ the limit of interest may now finally be obtained as follows.

**Theorem 4.7.** *Let $\mathcal{A}_\alpha$, $I_u(u)$ and $I_w(w)$ be given by (4.16), (4.19) and (4.20) respectively. Define the function $f(\alpha)$ as*

$$f(\alpha) \triangleq \inf_{(u,w) \in \mathcal{A}_\alpha} \left[ I_u(u) + I_w(w) \right] \tag{4.21}$$

*and let $g(a) \triangleq af(a)$. Then*

$$\lim_{m \to \infty} \frac{1}{m} \ln \mathrm{P}\left( z_m \geq a \right) = -g(a).$$

*Proof:* The proof is given in Appendix 4.A.6.

Theorem 4.7 together with Theorem 4.4 establish the existence of the rate $\gamma$. An interesting and immediate consequence of the result that

$$C(m) \doteq e^{\gamma m}$$

is that the probability that the number of nodes, $N$, visited by the sphere decoder is substantially larger than its expected value, tends to zero as $m$ grows. To see this note that for $\epsilon > 0$,

$$\mathrm{P}\left(N \geq e^{(\gamma+\epsilon)m}\right) \leq \frac{\mathrm{E}\{N\}}{e^{(\gamma+\epsilon)m}} = \frac{C(m)}{e^{(\gamma+\epsilon)m}} \doteq e^{-\epsilon m}, \tag{4.22}$$

by the Marcov inequality [Dur96]. Thus, for the system which has been considered it can be argued that it does make more sense to study the asymptotic expression for the expected complexity rather than the worst case complexity. Still, for finite $m$ the worst case complexity of the algorithm may be significantly larger than the expected complexity. This is further investigated in Section 5.3.

### 4.3.2 Computing the Asymptotic Rate in Practice

In Section 4.3.1 the existence of the asymptotic rate, $\gamma$, such that

$$C(m) \doteq e^{\gamma m}$$

is proven. Also, a way of computing this $\gamma$ is obtained. In this section a few words will be said about the practical aspects of this computation. Some numerical examples to show how $\gamma$ depends on parameters such as the SNR, $\rho$, and constellation, $\mathcal{S}$, are given in the following section. To recall the result of the previous section, the computation of $\gamma$ can be outlined as follows.

1. Let $I_w(w)$ be given by

$$I_w(w) = w - 1 - ln(w) \tag{4.23}$$

and compute $I_u(u)$ by numerically maximizing

$$I_u(u) = \sup_{\lambda} \left[ \lambda u - \ln \left( \frac{1}{|\mathcal{S}|^2} \sum_{s,\hat{s}\in\mathcal{S}} e^{\frac{\lambda}{2}|s-\hat{s}|^2} \right) \right] \tag{4.24}$$

over $\lambda \in \mathbb{R}$.

2. Compute $g(a) = af(a)$ by solving

$$f(a) = \inf_{(u,w)\in\mathcal{A}_a} [I_u(u) + I_w(w)] \tag{4.25}$$

where

$$\mathcal{A}_\alpha \triangleq \{(u,w) \mid (2\rho\alpha^2 u + \alpha)w \leq \kappa\}.$$

3. Compute $\gamma$ as in Theorem 4.4 by

$$\gamma = \sup_{a \in [0,1]} (a \ln |\mathcal{S}| - g(a)). \tag{4.26}$$

While daunting at first there are several properties of the functions and sets in the above which enables the computation of $\gamma$ in practice. First of all, from the proof of Lemma 4.8 in Appendix 4.A.6 it follows that if $(2\rho a^2 + a) \leq \kappa$ then $f(a)$ and $g(a)$ are identically equal to zero. Since

$$(2\rho a^2 + a) \leq \kappa \Leftrightarrow a \leq \frac{\sqrt{8\rho\kappa + 1} - 1}{4\rho} \triangleq \mu$$

for $a > 0$ it is known that $g(a) = 0$ in the range $a = [0, \mu]$. From (4.26) it therefore follows that an analytical lower bound on $\gamma$ is given by

$$\gamma \geq \frac{\sqrt{8\rho\kappa + 1} - 1}{4\rho} \ln |\mathcal{S}|. \tag{4.27}$$

This bound is however not tight for any $\rho$ or constellations $\mathcal{S}$. In other words, the supremum of (4.26) is achieved for some $a > \mu$. However, by Lemma 4.8 it is known that $g(a)$ is uniformly continuous in $a \in [0, 1]$ and this supremum is easily computed numerically.

Also, from Lemma 4.8 it is known that for $a > \mu$ the infimum of (4.25) is achieved on the boundary of $\mathcal{A}_a$ given by $(2\rho a^2 u + a)w = \kappa$ for some $u < 1$ and $w < 1$. Thus, by parametrization $f(a)$ can be computed by numerically minimizing $I_u(u) + I_w(w)$ over $u$ and $w$ where

$$\max\left(0, \frac{\kappa - a}{2\rho a^2}\right) \leq u \leq 1$$

and

$$w = w(u) = \frac{\kappa}{(2\rho a^2 u + a)}.$$

This is a one-dimensional optimization problem. There is however unfortunately no guarantee that the criterion function is unimodal given this parametrization of $u$ and $w$. Still, numerical experience suggests that this does not pose any serious problems in practise.

Finally, by the theory in [DZ98] it can be shown that the function $I_u(u)$ satisfies $I_u(0) = \ln |\mathcal{S}|$, $I_u(1) = 0$. Further, for $u \in (0, 1)$ the criterion function of (4.24) is concave and has a unique maximum for some $\lambda < 0$ which makes the computation of $I_u(u)$ easy.

For the numerical examples in the following section the computation of $I_u(u)$ is performed using a Newton approach while the optimizations in (4.25) and (4.26) are solved using a grid search combined with a golden section search to increase the accuracy.

### 4.3.3 Examples

To investigate the effect of $\mathcal{S}$ and $\rho$ on the rate $\gamma$ some numerical examples are included. To limit the number of possible scenarios the constant $\kappa$ of (4.9) will in this section be fixed to 1. Note, as before, that this is the case when the radius, $r$, is chosen such that

$$\mathrm{P}\left(\|\mathbf{x} - \mathbf{Rs}\| \leq r^2\right) = 1 - \epsilon$$

for some $\epsilon \in (0, 1)$ which is the strategy of choosing $r$ proposed in [HV02].

The analytical results of Section 4.3.1 along with the theory of Section 4.3.2 were used to compute the rate $\bar{\gamma}$ given by

$$\bar{\gamma} \triangleq \lim_{m\to\infty} \frac{1}{m} \log_{|\mathcal{S}|} C(m).$$

Note that $\bar{\gamma}$ relates to $\gamma$ as $\gamma = \ln|\mathcal{S}|\bar{\gamma}$. The normalized rate $\bar{\gamma}$ was chosen over $\gamma$ since it is always in the range $[0, 1]$ and thus gives a direct measure of the improvement offered by the sphere decoder over the full search, i.e.

$$C(m) \doteq |\mathcal{S}|^{\bar{\gamma}m} \leq |\mathcal{S}|^m.$$

Thus, $\bar{\gamma}$ can be interpreted as a reduction of the original problem size of $m$ to a subproblem of size $\bar{\gamma}m$ which is exhaustively searched by the sphere decoder.

The scenarios of $\mathcal{S}$ corresponding to 4-QAM, 8-PSK and 16-QAM were considered. The channel matrix was chosen according to the i.i.d. Rayleig fading channel model of Section 2.1.3. The results are shown in Figures 4.2, 4.3 and 4.4 where the analytical lower bound on $\bar{\gamma}$,

$$\bar{\mu} = \frac{\sqrt{8\rho + 1} - 1}{4\rho},$$

from (4.27) is included for reference. As can be seen the value of $\bar{\gamma}$ is always strictly above the bound given by $\bar{\mu}$. Typically, the larger the constellation is the loser the bound. Also, not surprisingly, as the SNR, $\rho$, is increased the value of $\bar{\gamma}$ is decreased and the sphere decoder become more efficient. This has previously been recognized in the literature

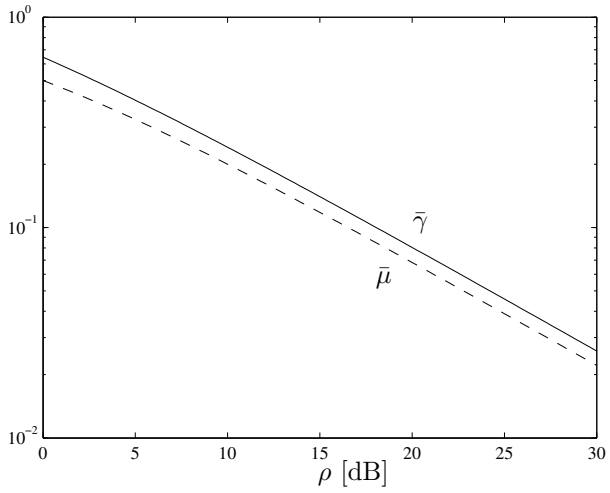


**Figure 4.2:** The normalized rate $\bar{\gamma}$ and analytic lower bound $\bar{\mu}$ as a function of SNR for the case where $\mathcal{S}$ is a 4-QAM constellation

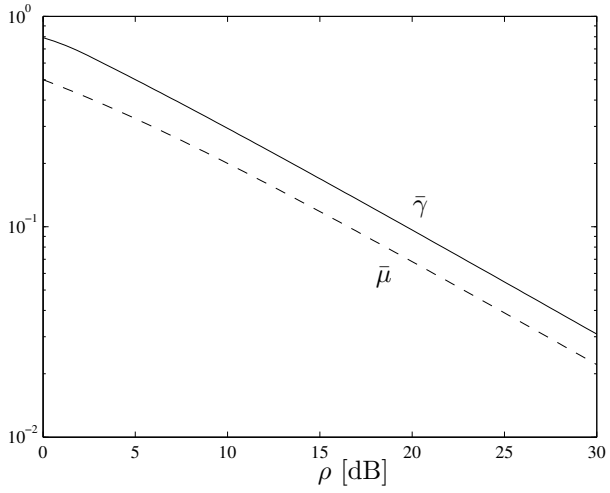


**Figure 4.3:** The normalized rate $\bar{\gamma}$ and analytic lower bound $\bar{\mu}$ as a function of SNR for the case where $\mathcal{S}$ is a 8-PSK constellation

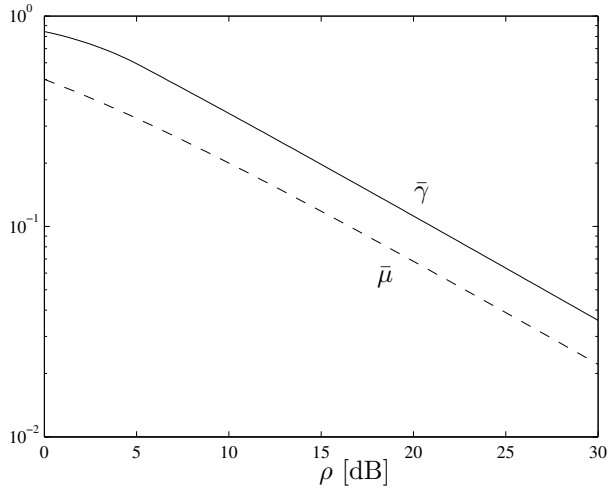


**Figure 4.4:** The normalized rate $\bar{\gamma}$ and analytic lower bound $\bar{\mu}$ as a function of SNR for the case where $\mathcal{S}$ is a 16-QAM constellation

[HV02, DAML01]. Note that the interpretation of the figures is that for an SNR of $\rho = 20$dB, where $\bar{\gamma} \approx 10^{-1}$, roughly 10 times as large problems can be solved if the sphere decoder is applied instead of the full search.

# Appendix 4.A Proofs

## 4.A.1 Proof of Theorem 4.1

*Proof:* The idea behind the proof is to show that with a high probability all constellation points are far away from the received point, $\mathbf{x} = \mathbf{Q}^{\mathrm{H}}\mathbf{y}$. To this end choose some $\kappa \in (0, |\mathcal{S}|^{-1})$ and $\epsilon > 0$ such that $\kappa|\mathcal{S}|e^{\epsilon} < 1$. Let $\mathcal{V}_m$ be the set vectors in $\mathbb{C}^m$ which are close to a constellation point, i.e.

$$\mathcal{V}_m \triangleq \{\mathbf{x} \in \mathbb{C}^m \mid \exists \hat{\mathbf{s}} \in \mathcal{S}^m \ \|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|^2 \leq \kappa\sigma^2 m\}$$

and note that $\mathbf{x} \in \mathcal{V}_m$ is equivalent to the statement

$$\|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}_{\mathrm{ML}}\|^2 \leq \kappa\sigma^2 m.$$

Since the set $\mathcal{V}_m$ is the union of $|\mathcal{S}|^m$ spheres in $\mathbb{C}^m$ of squared radius $r^2 = \kappa\sigma^2 m$ the volume of $\mathcal{V}_m$ may be upper bounded as

$$\mathrm{vol}(\mathcal{V}_m) \leq \frac{\pi^m(\kappa\sigma^2 m)^m}{\Gamma(m+1)}|\mathcal{S}|^m$$

where the first term in the product is the volume of one such sphere. Also, let $\mathcal{M}_m$ be defined by

$$\mathcal{M}_m \triangleq \{\mathbf{x} \in \mathbb{C}^m \mid \|\mathbf{x} - \mathbf{R}\mathbf{s}\|^2 \geq \sigma^2(1-\epsilon)m\}$$

where $\mathbf{s} \in \mathcal{S}^m$ is the transmitted message. Since $\mathrm{E}\left\{\|\mathbf{x} - \mathbf{R}\mathbf{s}\|^2\right\} = \mathrm{E}\left\{\|\mathbf{Q}^{\mathrm{H}}\mathbf{v}\|^2\right\} = \sigma^2 m$ and $\|\mathbf{Q}^{\mathrm{H}}\mathbf{v}\|^2$ is the sum of $m$ i.i.d. random variables it follows from the law of large numbers that

$$\lim_{m\to\infty} \mathrm{P}\left(\mathbf{x} \in \mathcal{M}_m^c\right) = 0.$$

Now consider the probability density function of $\mathbf{x}$, i.e.

$$f_{\mathbf{x}}(\mathbf{x}) = \frac{1}{(\pi\sigma^2)^m} e^{-\frac{1}{\sigma^2}\|\mathbf{x} - \mathbf{R}\hat{\mathbf{s}}\|^2}.$$

For any $\mathbf{x} \in \mathcal{M}_m$ the density may be bounded as

$$f_{\mathbf{x}}(\mathbf{x}) \leq \frac{1}{(\pi\sigma^2)^m} e^{-(1-\epsilon)m} \triangleq \bar{f}_{\mathbf{x}}.$$

Thus

$$\mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m \cap \mathcal{M}_m\right) \leq \bar{f}_{\mathbf{x}}\mathrm{vol}(\mathcal{V}_m) \leq (\kappa|\mathcal{S}|e^{\epsilon})^m \frac{m^m e^{-m}}{\Gamma(m+1)}.$$

However, since by Stirling's approximation formula [Dur96]

$$\lim_{m\to\infty} \frac{m^m e^{-m}\sqrt{2\pi m}}{\Gamma(m+1)} = 1$$

and since $(\kappa|\mathcal{S}|e^{\epsilon}) < 1$ by assumption it follows that

$$\lim_{m\to\infty} \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m \cap \mathcal{M}_m\right) = 0.$$

Therefore, by using

$$\mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m\right) = \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m \cap \mathcal{M}_m\right) + \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m \cap \mathcal{M}_m^c\right)$$

together with

$$\mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m \cap \mathcal{M}_m^c\right) \leq \mathrm{P}\left(\mathbf{x} \in \mathcal{M}_m^c\right) \to 0$$

it follows that

$$\lim_{m\to\infty} \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m\right) = 0$$

and

$$\lim_{m\to\infty} \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m^c\right) = 1. \tag{4.28}$$

This means that the closest constellation point, $\mathbf{R}\hat{\mathbf{s}}_{\mathrm{ML}}$, will lie at least a squared distance of $\kappa\sigma^2 m$ away from the received point, $\mathbf{x}$, with a probability which tends to 1 as $m$ grows. Also, if the sphere decoder solves the ML detection problem when the event $\mathcal{V}_m^c$ is true the squared radius must be at least $\kappa\sigma^2 m$ by the definition of $\mathcal{V}_m$, i.e.

$$\mathcal{D}_m \cap \left(\mathbf{x} \in \mathcal{V}_m^c\right) \Rightarrow r_m^2 \geq \kappa\sigma^2 m.$$

Therefore it follows that

$$\begin{aligned}
&\mathrm{P}\left(r_m^2 \geq \kappa\sigma^2 m\right) \\
\geq &\mathrm{P}\left(\mathcal{D}_m \cap \left(\mathbf{x} \in \mathcal{V}_m^c\right)\right) \\
= &\mathrm{P}\left(\mathcal{D}_m\right) + \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m^c\right) - \mathrm{P}\left(\mathcal{D}_m \cup \left(\mathbf{x} \in \mathcal{V}_m^c\right)\right) \\
\geq &\mathrm{P}\left(\mathcal{D}_m\right) + \mathrm{P}\left(\mathbf{x} \in \mathcal{V}_m^c\right) - 1
\end{aligned}$$

which, due to (4.28) and the assumption about $\mathrm{P}\left(\mathcal{D}_m\right)$, implies that

$$\liminf_{m\to\infty} \mathrm{P}\left(r_m^2 \geq \kappa\sigma^2 m\right) \geq \nu.$$

This concludes the proof. ■

### 4.A.2 Proof of Lemma 4.2

*Proof:* Let, for $\bar{\mathbf{s}} \in \mathcal{S}^k$,

$$1_{\mathcal{R}_k}(\bar{\mathbf{s}}) = \begin{cases} 1 & \bar{\mathbf{s}} \in \mathcal{R}_k \\ 0 & \bar{\mathbf{s}} \notin \mathcal{R}_k \end{cases}$$

be the indicator function for the set $\mathcal{R}_k$. Further, let $N = N(\mathbf{H}, \mathbf{y})$ be the number of nodes visited in the search tree for a given $\mathbf{H}$ and $\mathbf{y}$. Then, $N$ may be computed by summing over all nodes using $1_{\mathcal{R}_k}(\bar{\mathbf{s}})$ to count only nodes which are included in the search. Thus

$$\begin{aligned}
N &= \sum_{k=0}^{m} \sum_{\bar{\mathbf{s}} \in \mathcal{S}^k} 1_{\mathcal{R}_k}(\bar{\mathbf{s}}) \\
&= \sum_{k=0}^{m} |\mathcal{S}|^{-(m-k)} \sum_{\tilde{\mathbf{s}} \in \mathcal{S}^{m-k}} \sum_{\bar{\mathbf{s}} \in \mathcal{S}^k} 1_{\mathcal{R}_k}(\bar{\mathbf{s}}) \\
&= \sum_{k=0}^{m} |\mathcal{S}|^{-(m-k)} \sum_{\hat{\mathbf{s}} \in \mathcal{S}^m} 1_{\mathcal{R}_k}(\hat{\mathbf{s}}_{\iota_k}) \\
&= \sum_{\hat{\mathbf{s}} \in \mathcal{S}^m} |\mathcal{S}|^{-m} \sum_{k=0}^{m} |\mathcal{S}|^k 1_{\mathcal{R}_k}(\hat{\mathbf{s}}_{\iota_k}) \\
&= \sum_{\hat{\mathbf{s}} \in \mathcal{S}^m} |\mathcal{S}|^{-m} \sum_{k=0}^{d(\hat{\mathbf{s}})} |\mathcal{S}|^k \\
&= \sum_{\hat{\mathbf{s}} \in \mathcal{S}^m} |\mathcal{S}|^{-m} \frac{|\mathcal{S}|^{d(\hat{\mathbf{s}})+1} - 1}{|\mathcal{S}| - 1}
\end{aligned}$$

where the otherwise ill-defined terms corresponding to $k = 0$ and $k = m$ are conveniently defined as

$$\sum_{\bar{\mathbf{s}} \in \mathcal{S}^0} 1_{\mathcal{R}_0}(\bar{\mathbf{s}}) \triangleq 1$$

and

$$\sum_{\tilde{\mathbf{s}} \in \mathcal{S}^0} \sum_{\bar{\mathbf{s}} \in \mathcal{S}^m} 1_{\mathcal{R}_m}(\mathbf{s}_{\iota_m}) \triangleq \sum_{\bar{\mathbf{s}} \in \mathcal{S}^m} 1_{\mathcal{R}_m}(\mathbf{s}_{\iota_m}).$$

Note that the last line equals

$$N = \frac{\mathrm{E}_{\hat{\mathbf{s}}} \left\{ |\mathcal{S}|^{d(\hat{\mathbf{s}})+1} \right\} - 1}{|\mathcal{S}| - 1}$$

for a random variable, $\hat{\mathbf{s}}$, uniformly distributed over $\mathcal{S}^m$. Therefore, since by definition

$$C \triangleq \mathrm{E}_{\mathbf{H},\mathbf{y}}\left\{N\right\},$$

the expected complexity may be computed as

$$C = \frac{\mathrm{E}\left\{|\mathcal{S}|^{d+1}\right\} - 1}{|\mathcal{S}| - 1}$$

where expectation is taken over $\mathbf{H}$, $\mathbf{x}$ and $\hat{\mathbf{s}}$. This concludes the proof. ■

### 4.A.3 Proof of Theorem 4.3

*Proof:* Let $\mathcal{R}$ be the event that $r^2 \geq \kappa\sigma^2 m$, then

$$\mathrm{E}\left\{|\mathcal{S}|^{d+1}\right\} = \nu\mathrm{E}\left\{|\mathcal{S}|^{d+1}|\mathcal{R}\right\} + (1-\nu)\mathrm{E}\left\{|\mathcal{S}|^{d+1}|\mathcal{R}^c\right\} \geq \nu\mathrm{E}\left\{|\mathcal{S}|^{d+1}|\mathcal{R}\right\}.$$

Due to the convexity of $|\mathcal{S}|^{d+1}$ it follows by Jensen's inequality [Ro] that

$$\mathrm{E}\left\{|\mathcal{S}|^{d+1}|\mathcal{R}\right\} \geq |\mathcal{S}|^{\mathrm{E}\{d|\mathcal{R}\}+1}. \tag{4.29}$$

In light of the above what needs to be proven is that

$$\mathrm{E}\left\{d|\mathcal{R}\right\} \geq \eta m - 1.$$

To this end note that the probability that $d$ is strictly smaller than some $k$ is given by

$$\mathrm{P}\left(d < k|\mathcal{R}\right) = \mathrm{P}\left(||\mathbf{p}_{\iota_k}||^2 > r^2|\mathcal{R}\right) \leq \mathrm{P}\left(||\mathbf{p}_{\iota_k}||^2 > \kappa\sigma^2 m|\mathcal{R}\right)$$

where $\mathbf{p} \triangleq \mathbf{x} - \mathbf{R}\hat{\mathbf{s}}$. The Markov inequality [Dur96] upper bounds this probability as

$$\mathrm{P}\left(||\mathbf{p}_{\iota}||^2 > \kappa\sigma^2 m|\mathcal{R}\right) \leq \frac{\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2|\mathcal{R}\right\}}{\kappa\sigma^2 m}.$$

Note also that since

$$\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2\right\} = \nu\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2|\mathcal{R}\right\} + (1-\nu)\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2|\mathcal{R}^c\right\}$$

it follows that

$$\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2|\mathcal{R}\right\} \leq \nu^{-1}\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2\right\}.$$

The probability that the depth $d$ is at least as large as $k$ can thus be lower bounded by

$$\mathrm{P}\left(d \geq k|\mathcal{R}\right) \geq 1 - \frac{\mathrm{E}\left\{||\mathbf{p}_{\iota_k}||^2\right\}}{\nu\kappa\sigma^2 m}. \tag{4.30}$$

Since $\mathbf{R}$, $\mathbf{s}$, $\hat{\mathbf{s}}$, and $\mathbf{v}$ are assumed independent, the expected value can be computed as

$$\begin{aligned}
&\mathrm{E}\left\{\|\mathbf{p}_{\iota_k}\|^2\right\} = \mathrm{E}\left\{\|\mathbf{R}_{\iota_k}(\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k}) + [\mathbf{Q}^{\mathrm{H}}\mathbf{v}]_{\iota_k}\|^2\right\} \\
=&\mathrm{E}\left\{\|\|\mathbf{R}_{\iota_k}(\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k})\|^2\right\} + \mathrm{E}\left\{\|[\mathbf{Q}^{\mathrm{H}}\mathbf{v}]_{\iota_k}\|^2\right\} \\
=&\sum_{i=m-k+1}^{m} \mathrm{E}\left\{|s_i - \hat{s}_i|^2\right\} \mathrm{E}\left\{\|[\mathbf{r}_i]_{\iota_k}\|^2\right\} + k\sigma^2
\end{aligned} \tag{4.31}$$

where $\mathbf{r}_i$ is the $i$:th column of $\mathbf{R}$ and where $s_i$ and $\hat{s}_i$ are the $i$:th components of $\mathbf{s}$ and $\hat{\mathbf{s}}$ respectively. Since both $s_i$ and $\hat{s}_i$ are assumed independent and uniformly distributed on $\mathcal{S}$ and satisfy $\mathrm{E}\left\{s_i\right\} = \mathrm{E}\left\{\hat{s}_i\right\} = 0$,

$$\mathrm{E}\left\{|s_i - \hat{s}_i|^2\right\} = 2\mathrm{E}\left\{|s_i|^2\right\}. \tag{4.32}$$

Since $\mathbf{r}_i = \mathbf{Q}^{\mathrm{H}}\mathbf{h}_i$ where $\mathbf{h}_i$ is the $i$:th column of $\mathbf{H}$ it follows that

$$\mathrm{E}\left\{\|[\mathbf{r}_i]_{\iota_k}\|^2\right\} \leq \mathrm{E}\left\{\|\mathbf{h}_i\|^2\right\}. \tag{4.33}$$

Using

$$\mathrm{E}\left\{\|\mathbf{h}_i\bar{s}_i\|^2\right\} = \mathrm{E}\left\{\|\mathbf{h}_i\|^2\right\} \mathrm{E}\left\{|s_i|^2\right\}$$

together with (4.32) and (4.33) yields

$$\mathrm{E}\left\{|s_i - \hat{s}_i|^2\right\} \mathrm{E}\left\{\|[\mathbf{r}_i]_{\iota_k}\|^2\right\} \leq 2\rho_s\sigma^2.$$

The expression of (4.31) can thus be bounded by

$$\mathrm{E}\left\{\|\mathbf{p}_{\iota_k}\|^2\right\} \leq k\sigma^2(2\rho_s + 1).$$

Using the above, the probability that $d$ is greater than or equal to $k$ can be bounded as

$$\mathrm{P}\left(d \geq k|\mathcal{R}\right) \geq 1 - \frac{k(2\rho_s + 1)}{\nu\kappa m} \geq 1 - \frac{k}{K}$$

for

$$K \triangleq \left\lfloor \frac{\nu\kappa m}{2\rho_s + 1} \right\rfloor$$

Thus, by noting that $K \leq m$,

$$\mathrm{E}\left\{d|\mathcal{R}\right\} = \sum_{k=1}^{m} \mathrm{P}\left(d \geq k|\mathcal{R}\right) \geq \sum_{k=1}^{K} \mathrm{P}\left(d \geq k|\mathcal{R}\right) \geq \sum_{k=1}^{K} \left(1 - \frac{k}{K}\right) = \frac{K-1}{2}.$$

However, since

$$K \geq \frac{\nu\kappa m}{2\rho_s + 1} - 1$$

it follows that

$$\mathrm{E}\left\{d|\mathcal{R}\right\} \geq \frac{K-1}{2} \geq \frac{\nu\kappa m}{4\rho_s + 2} - 1.$$

Letting

$$\eta = \frac{\nu\kappa}{4\rho_s + 2} \tag{4.34}$$

and using (4.29), (4.34) together with Lemma 4.2 concludes the proof. ■

### 4.A.4 Proof of Theorem 4.4

The proof is divided into two parts, one which established a lower bound on the form

$$\liminf_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \geq \sup_{0\leq a\leq 1} \left(a \ln |\mathcal{S}| - g(a)\right)$$

and a second part which gives the upper bound

$$\limsup_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \leq \sup_{0\leq a\leq 1} \left(a \ln |\mathcal{S}| - g(a)\right).$$

The lower bound is somewhat easier to prove. To this end note that for any $a \in [0, 1]$ it holds that

$$\begin{aligned}\mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} &= \int_{[0,1]} |\mathcal{S}|^{mz_m} \mathrm{P}\left(dz_m\right) \\ &\geq \int_{[a,1]} |\mathcal{S}|^{mz_m} \mathrm{P}\left(dz_m\right) \geq |\mathcal{S}|^{ma} \mathrm{P}\left(z_m \geq a\right)\end{aligned}$$

which implies

$$\begin{aligned}&\liminf_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \\ &\geq \liminf_{m\to\infty} \left(a \ln |\mathcal{S}| + \frac{1}{m} \ln \mathrm{P}\left(z_m \geq a\right)\right) = a \ln |\mathcal{S}| - g(a).\end{aligned}$$

However, since $a \in [0,1]$ was arbitrary it follows that

$$\liminf_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \geq \sup_{0\leq a\leq 1} \left(a \ln |\mathcal{S}| - g(a)\right)$$

which establishes the lower bound.

In order to prove the upper bound consider the following. Given $\epsilon > 0$, choose some $N$, and $a_n$, $n = 1, \ldots, N$, such that $a_1 = 0$, $a_N = 1$, $a_n \leq a_{n+1}$ and $a_{n+1} \leq a_n + \epsilon$ for $n = 1, \ldots, N$. Note that this can be done for any $\epsilon > 0$. Let $\mathcal{F}_n = [a_n, a_{n+1})$ for $n = 1, \ldots, N-2$ and $\mathcal{F}_{N-1} = [a_{N-1}, a_N]$ which implies

$$\cup_{n=1}^{N-1} \mathcal{F}_n = [0,1] \qquad \text{and} \qquad \mathcal{F}_i \cap \mathcal{F}_j = \emptyset \quad i \neq j.$$

Then

$$\begin{aligned}
&\mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} = \int_{[0,1]} |\mathcal{S}|^{mz_m} \mathrm{P}\left(dz_m\right) = \sum_{n=1}^{N-1} \int_{\mathcal{F}_n} |\mathcal{S}|^{mz_m} \mathrm{P}\left(dz_m\right) \\
\leq &\sum_{n=1}^{N-1} |\mathcal{S}|^{ma_{n+1}} \mathrm{P}\left(z_m \in \mathcal{F}_n\right) \leq \sum_{n=1}^{N-1} |\mathcal{S}|^{m(a_n+\epsilon)} \mathrm{P}\left(z_m \geq a_n\right) \\
\leq &N \max_{1\leq n<N} |\mathcal{S}|^{m(a_n+\epsilon)} \mathrm{P}\left(z_m \geq a_n\right).
\end{aligned}$$

Using the above

$$\begin{aligned}
&\limsup_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \\
\leq &\limsup_{m\to\infty} \left(\frac{\ln N}{m} + \max_{1\leq n<N} \left((a_n+\epsilon)\ln|\mathcal{S}| + \frac{1}{m}\ln \mathrm{P}\left(z_m \geq a_n\right)\right)\right) \\
\leq &\max_{1\leq n<N} \left((a_n+\epsilon)\ln|\mathcal{S}| - g(a_n)\right) \leq \sup_{0\leq a\leq 1} \left(a\ln|\mathcal{S}| - g(a)\right) + \epsilon \ln|\mathcal{S}|.
\end{aligned}$$

Since $\epsilon > 0$ was arbitrary it follows that

$$\limsup_{m\to\infty} \frac{1}{m} \ln \mathrm{E}\left\{|\mathcal{S}|^{mz_m}\right\} \leq \sup_{0\leq a\leq 1} \left(a \ln |S| - g(a)\right)$$

which established the upper bound and concludes the proof. ■

### 4.A.5 Proof of Theorem 4.5

To begin, note that

$$\mathrm{P}\left(z_m \geq a\right) = \mathrm{P}\left(d \geq ma\right) = \mathrm{P}\left(d \geq \lceil ma \rceil\right)$$

where the last equality follows since $d$ is integer valued. Now, let $k = \lceil ma \rceil$ and note that

$$\mathrm{P}\left(d \geq k\right) = \mathrm{P}\left(\|\mathbf{p}_{\iota_k}\|^2 \leq r_m^2\right).$$

One of the results derived in [HV03] are that while $\|\mathbf{p}_{\iota_k}\|^2$ is generally not equal to $\|\mathbf{H}_{\iota_k}(\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k}) + \mathbf{v}_{\iota_k}\|^2$ they have the same distribution for the i.i.d. Rayleigh fading channel. Using this result the above probability may written as

$$\mathrm{P}\left(d \geq k\right) = \mathrm{P}\left(\|\mathbf{p}_{\iota_k}\|^2 \leq r_m^2\right) = \mathrm{P}\left(\|\mathbf{H}_{\iota_k}(\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k}) + \mathbf{v}_{\iota_k}\|^2 \leq r_m^2\right).$$

By noting that $\mathbf{H}_{\iota_k}(\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k}) + \mathbf{v}_{\iota_k}$ is a Gaussian vector for fixed $\mathbf{s}$ and $\hat{\mathbf{s}}$ it can be be seen [HV03] that

$$\mathrm{P}\left(z_m \geq a\right) = \mathrm{P}\left(\left(\frac{\|\mathbf{s}_{\iota_k} - \hat{\mathbf{s}}_{\iota_k}\|^2}{m} + \sigma^2\right)\|\mathbf{q}_{\iota_k}\|^2 \leq r_m^2\right)$$

where $\mathbf{q} \in \mathbb{C}^m$ is vector of i.i.d. Gaussian elements of unit variance. To simplify the expression further the following definitions are introduced as in the theorem.

$$w_k \triangleq \frac{1}{k}\sum_{i=1}^{k} |q_i|^2 \tag{4.35}$$

and

$$u_k \triangleq \frac{1}{k}\sum_{i=1}^{k} \frac{|s_i - \hat{s}_i|^2}{2} \tag{4.36}$$

where $q_i$ are i.i.d. zero-mean normally distributed with unit variance and where $s_i$ and $\hat{s}_i$ are i.i.d. uniformly distributed over $\mathcal{S}$. The normalizations are chosen such that $\mathrm{E}\left\{w_k\right\} = 1$ and $\mathrm{E}\left\{u_k\right\} = 1$ and thus both $u_k$ and $w_k$ converge in probability to 1 due to the weak law of large numbers. Using the above definition the probability, $\mathrm{P}\left(z_m \geq a\right)$, may be written as

$$\begin{aligned}\mathrm{P}\left(z_m \geq a\right) =& \mathrm{P}\left(\left(\frac{2ku_k}{m} + \sigma^2\right)kw_k \leq r_m^2\right)\\ =& \mathrm{P}\left(\left(2\rho\frac{k}{m}u_k + 1\right)\frac{\kappa\sigma^2 k}{r_m^2}w_k \leq \kappa\right)\end{aligned}$$

where $\rho = \sigma^{-2}$ has been used for the last equality.

Now introduce the function $P(\alpha, k)$ as

$$P(\alpha, k) \triangleq \mathrm{P}\left(\left(2\rho\alpha^2 u_k + \alpha\right)w_k \leq \kappa\right).$$

Due to the equality $k = \lceil am \rceil$, and by the assumption on $r_m^2$ given in (4.9) it follows that

$$\lim_{m\to\infty} \frac{k}{m} = \lim_{m\to\infty} \frac{\kappa\sigma^2 k}{r_m^2} = a.$$

Therefore it can be seen from (**??**) that for any $\alpha > a$ there is an $M$ such that

$$\mathrm{P}\left(z_m \geq a\right) \geq P(\alpha, \lceil ma \rceil)$$

for $m \geq M$. Similarly, for any $\alpha < a$ there is an $M$ such that

$$\mathrm{P}\left(z_m \geq a\right) \leq P(\alpha, \lceil ma \rceil)$$

for $m \geq M$. ■

### 4.A.6 Proof of Theorem 4.7

Before establishing Theorem 4.7 it is useful to prove continuity of the function $f(\alpha)$ given by (4.21). This is established by the lemma below.

**Lemma 4.8.** *Let the set $\mathcal{A}_\alpha$ be given as in (4.16) and define the function $f(\alpha)$ as*

$$f(\alpha) \triangleq \inf_{(u,w)\in\mathcal{A}_\alpha} [I_u(u) + I_w(w)]. \tag{4.37}$$

*Then, given $\rho, \kappa > 0$, the function $f(\alpha)$ is uniformly continuous over $\alpha \in [0, 1]$.*

*Proof (of Lemma 4.8):* In order to prove the lemma some properties of $I_u(u)$ and $I_w(w)$ must be obtained. From the closed form expression of $I_w(w)$ it can be seen that the function is continuous for $w > 0$. Further $I_w(w)$ is convex, nonnegative and attains a unique minimum equal to 0 for $w = 1$. The function is also decreasing in the range $(0, 1]$. While lacking a closed form expression, the function $I_u(u)$ can be proven to have similar properties. Since $I_u(u)$ is the rate function for a sum of i.i.d. variables it is a nonnegative convex function [DZ98] and convergence of $u_k$ to 1 implies that $I_u(u)$ attains a unique minimum equal to 0 for $u = 1$. Further, since $u_1$ belong to a finite alphabet, $\mathrm{P}\left(u_1 = 0\right) > 0$ and $\mathrm{P}\left(u_1 \geq 1\right) > 0$, it follows that $I_u(u)$ is continuous on the compact set $[0, 1]$ [DZ98]. This together with convexity implies that $I_u(u)$ must be a continuous, decreasing function in the range $u = [0, 1]$. Having obtained these properties of $I_u(u)$ and $I_w(w)$, the lemma can be successfully proven in what follows.

Now let $(u^\star, w^\star)$ be the optimizer of (4.37). Since both $I_u(u)$ and $I_w(w)$ are decreasing for $u, w \leq 1$ and attain minimums at 1 the optimizing $(u^\star, w^\star)$ must satisfy $u^\star \leq 1$ and $w^\star \leq 1$. Also,

$$(2\rho\alpha^2 u^\star + \alpha)w^\star = \kappa$$

if $(2\rho a^2 + a) \leq \kappa$, and $(u^\star, w^\star) = (1, 1)$ otherwise. Thus, for any given $u$, the $w$ which minimize the criterion of (4.37) is given by

$$w = w(u, \alpha) = \min\left(1, \frac{\kappa}{2\rho\alpha^2 u + \alpha}\right)$$

which is a continuous function over $(u, \alpha) \in \mathcal{D} \triangleq [0, 1] \times [0, 1]$. It further holds that

$$w(u, \alpha) \geq \min\left(1, \frac{\kappa}{2\rho + 1}\right) > 0$$

for any $(u, \alpha) \in \mathcal{D}$. Thus, since $I_w(w)$ is continious for $w > 0$, the function

$$h(u, \alpha) \triangleq I_u(u) + I_w(w(u, \alpha))$$

is a continious function over $\mathcal{D}$. Additionally, since $\mathcal{D}$ is compact, uniform continuity of $h(u, \alpha)$ follows [Rud96].

Using $h(u, \alpha)$, the function $f(\alpha)$ can be written as

$$f(\alpha) = \inf_{u \in [0,1]} h(u, \alpha). \tag{4.38}$$

The uniform continuity of $h(u, \alpha)$ implies that given $\delta > 0$ there is an $\epsilon > 0$ such that $|h(u, \alpha) - h(\bar{u}, \bar{\alpha})| < \delta$ whenever $|u - \bar{u}| < \epsilon$ and $|\alpha - \bar{\alpha}| < \epsilon$. Assume now that $\delta$ and $\epsilon$ are chosen as above and let $\alpha, \bar{\alpha}$ satisfy $|\alpha - \bar{\alpha}| < \epsilon$. Further let $u^\star$ and $\bar{u}^\star$ be the optimizing $u$ of (4.38) for $\alpha$ and $\bar{\alpha}$ respectively. Note that $u^\star$ and $\bar{u}^\star$ always exist due to the continuity of $h(u, \alpha)$ over the compact set $\mathcal{D}$. It is however not necessary that $|u^\star - \bar{u}^\star| < \epsilon$. Still,

$$f(\alpha) = h(u^\star, \alpha) \geq h(u^\star, \bar{\alpha}) - \delta \geq h(\bar{u}^\star, \bar{\alpha}) - \delta = f(\bar{\alpha}) - \delta$$

where the first inequality follows from the uniform continuity of $h(u, \alpha)$ and the second inequality follows since $\bar{u}^\star$ is the minimizer of (4.38) for $\bar{\alpha}$. By interchanging the roles of $\alpha$ and $\bar{\alpha}$ it similarly follows that

$$f(\bar{\alpha}) \geq f(\alpha) - \delta$$

which implies that given $\delta > 0$, there is an $\epsilon > 0$ such that

$$|f(\alpha) - f(\bar{\alpha})| < \delta$$

whenever $|a - \bar{a}| < \epsilon$. Thus, $f(\alpha)$ is uniformly continuous over $\alpha \in [0, 1]$ which is what was to be proven. ■

*Proof (of Theorem 4.7):* Since $\mathcal{A}_\alpha$ is closed it follows immediately from Theorem 4.6 and the definition of $f(a)$ in (4.37) that

$$\limsup_{k\to\infty} \frac{1}{k} \ln P(\alpha, k) = \limsup_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right) \leq -f(a).$$

Note that the technical condition of Theorem 4.6, i.e. $\Lambda(\boldsymbol{\lambda}) < \infty$ for some neighborhood of $\mathbf{0}$, is satisfied since

$$\Lambda(\boldsymbol{\lambda}) = \ln \mathrm{E}\left\{e^{\lambda_1 u_1}\right\} + \ln \mathrm{E}\left\{e^{\lambda_2 w_1}\right\}$$

where the first term on the right hand side is finite for any $\lambda_1 \in \mathbb{R}$ and the second term is finite for $\lambda_2 < 1$.

By the definition of $\mathcal{A}_\alpha$ in (4.16) it can be seen that $\mathcal{A}_{\bar{\alpha}} \subset \mathcal{A}_\alpha^o$ for any $\bar{\alpha} > \alpha$. Thus

$$\begin{aligned}
&\liminf_{k\to\infty} \frac{1}{k} \ln P(\alpha, k) = \liminf_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha\right) \\
&\geq \liminf_{k\to\infty} \frac{1}{k} \ln \mathrm{P}\left((u_k, w_k) \in \mathcal{A}_\alpha^o\right) \geq - \inf_{(u,w)\mathcal{A}_\alpha^o} [I_u(u) + I_w(w)] \\
&\geq - \inf_{(u,w)\in\mathcal{A}_{\bar{\alpha}}} [I_u(u) + I_w(w)] = -f(\bar{\alpha})
\end{aligned}$$

for any $\bar{\alpha} > \alpha$. By the continuity of $f(\alpha)$ given in Lemma 4.8 it follows that

$$\liminf_{k\to\infty} \frac{1}{k} \ln P(\alpha, k) \geq -f(\alpha).$$

Therefore, again noting that $k = \lceil ma \rceil$ implies

$$\lim_{m\to\infty} \frac{k}{m} = a$$

it follows by (4.13) that

$$\begin{aligned}
&\limsup_{m\to\infty} \frac{1}{m} \ln \mathrm{P}\left(z_m \geq a\right) = \limsup_{m\to\infty} \frac{a}{k} \ln \mathrm{P}\left(z_m \geq a\right) \\
&\leq \limsup_{k\to\infty} \frac{a}{k} \ln P(\alpha, k) = -af(\alpha)
\end{aligned}$$

for any $\alpha < a$. Similarly, by equation (4.12),

$$\begin{aligned}&\liminf_{m\to\infty} \frac{1}{m} \ln \mathrm{P}\left(z_m \geq a\right) = \liminf_{m\to\infty} \frac{a}{k} \ln \mathrm{P}\left(z_m \geq a\right) \\ \geq &\liminf_{k\to\infty} \frac{a}{k} \ln P(\alpha, k) = -af(\alpha)\end{aligned}$$

for any $\alpha > a$. However, since $\alpha$ may be arbitrarily close to $a$ and since $f(\alpha)$ is continuous in $\alpha \in [0, 1]$ by Lemma 4.8 it follows that

$$\lim_{m\to\infty} \frac{1}{m} \ln \mathrm{P}\left(z_m \geq a\right) = -af(a) = -g(a)$$

which concludes the proof. ■

# Chapter 5

# Numerical Evaluation

In this chapter the semidefinite relaxation based decoder and the sphere decoder are evaluated numerically by simulations. The data is generated according to a real valued version of the i.i.d. Rayleigh fading channel. The main motivation of this choice of channel is that it provides a scenario for which both the semidefinite relaxation (SDR) algorithm and the sphere decoder (SD) are directly applicable. Also, by considering such a simple scenario the result can easily be reproduced.

The details of the specific algorithm implementations used in this chapter are given in Appendix 5.A. Both the SDR and the SD algorithms are implemented in an efficient manner based on pseudo code available in the communications literature. While there of course is no way to guarantee that the implementations used are the best possible, a considerable amount of effort has been spent on efficient implementation and coding to reduce their complexity. For both algorithms, the input is considered to be $\mathbf{H}$ and $\mathbf{y}$ and the output is the estimate, $\hat{\mathbf{s}}$.

## 5.1 Data Model

In order to create scenarios where semidefinite relaxation and the sphere decoder can be compared directly attention is restricted to the case where the constellation is binary, i.e. $\mathcal{S} = \{\pm 1\}$. The channel matrix and noise are also real valued and the problem instances are generated according to

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{v}, \quad \text{for} \quad \mathbf{H} = \sqrt{\frac{\rho}{n}}\mathbf{G},$$

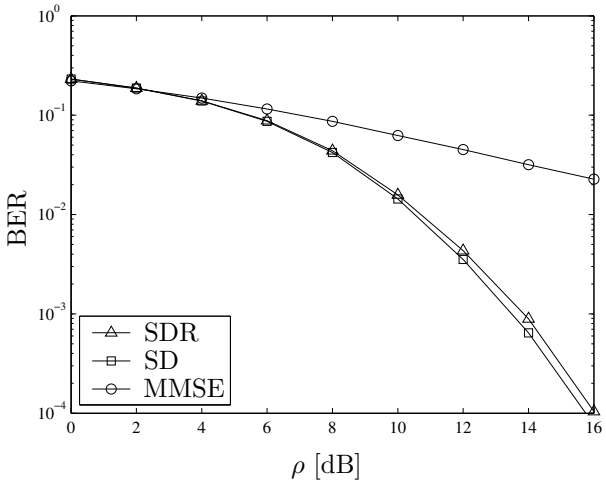


**Figure 5.1:** BER curves for the scenario where $m = 10$ and $n = 10$.

where the elements of $\mathbf{G} \in \mathbb{C}^{n \times m}$ and $\mathbf{v} \in \mathbb{C}^n$ are drawn independently from, zero mean, unit variance real valued Gaussian distribution. Note that the SNR, $\rho$, is given by

$$\rho = \frac{\mathrm{E}\left\{\|\mathbf{Hs}\|^2\right\}}{\mathrm{E}\left\{\|\Pi_{\mathbf{H}}\mathbf{v}\|^2\right\}}$$

as in (2.2) for this setup.

## 5.2 BER Performance

Figures 5.1 and 5.2 show the simulated bit error rate (BER) defined as the empirical estimate of $\mathrm{P}\left(\hat{s}_i \neq s_i\right)$ for a system of size $(n, m) = (10, 10)$ and $(n, m) = (20, 10)$ respectively. Each point on the curves was generated by averaging over $10^5$ Monte-Carlo trials. As a reference the BER of the MMSE detector is also included. While the superior performance of the near ML detectors are evident in the figures, it is interesting to note that as $n$ is increased to 20 the performance of the MMSE detector is significantly improved. This can be explained by that, on average, the condition number of the $20 \times 10$ matrix $\mathbf{H}$ is significantly better than that of the corresponding $10 \times 10$ matrix. This behavior of the

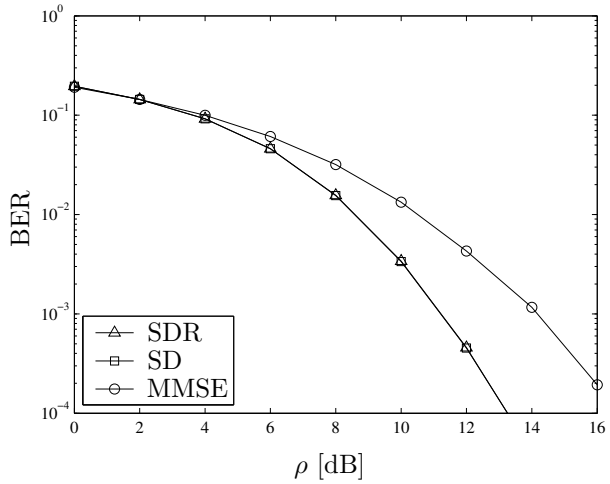


**Figure 5.2:** BER curves for the scenario where $m = 10$ and $n = 20$.

suboptimal detector, i.e. the problem to correctly detect the transmitted symbols when the channel matrix is poorly conditioned is well recognized in the literature, see e.g. [ASH03]. From Figure 5.1 it is seen that for the $10 \times 10$ scenario the sphere decoder has a slightly better performance than the SDR decoder. For the $20 \times 10$ case however, the difference is not even noticeable as is shown in Figure 5.2. A final remark is that in the generation of these plots the sphere decoder is started with an infinite initial radius, $r$, and therefore the sphere decoder provides the true ML estimate.

In Figure 5.3 the portion of instances for which the SDR detector attains a rank one solution is given as a function of the SNR for $10 \times 10$ case as well as the $20 \times 10$ case. The behavior of the SDR commented on in Chapter 3 can be seen in the figure. As the SNR increase or the conditioning of the channel matrix improves the probability of the rank one solutions increase. However, as can also be seen from Figure 5.3, for the $10 \times 10$ scenario the proportion of rank one solutions is still relatively low. Thus, if the method outlined in Section 3.2.1 is to be used, the channel needs to be relatively well conditioned. A reasonable scenario where this may be the case is in a CDMA system where typically the signatures, or spreading codes, of the users can be designed such that the cross correlation between different users is small. This in turn makes

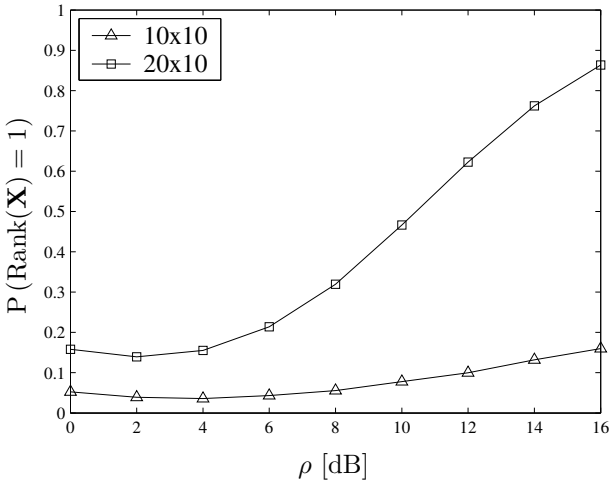


**Figure 5.3:** Probability of obtaining a rank one solution in the SDR algorithm as a function of SNR.

the resulting channel matrix closer to orthogonal which imply a smaller condition number.

## 5.3 Computational Complexity

By the analytic complexity results given in Chapters 3 and 4 it is known that for any SNR, $\rho > 0$, there will always be a problem size, $m$, where the semidefinite relaxation algorithm is of lower complexity than the sphere decoder. This is however an asymptotic statement and from the analytic results it is unclear for which size $m$ this transition occurs. It is likely that this will depend on the particular scenario under consideration.

In order to address this question for the scenario considered in this chapter the complexity of the SDR and the SD algorithms was investigated for square systems, i.e. $n = m$, generated by the data model given in Section 5.1. The SNR was fixed at $\rho = 10$dB which for the $10 \times 10$ system corresponds to a BER of just under $10^{-2}$. The initial radius, r, of the sphere decoder was chosen by the method proposed in [HV02] such that

$$\mathrm{P}\left(\|\mathbf{x} - \mathbf{R}\mathbf{s}\|^2 > r^2\right) = 10^{-3}$$

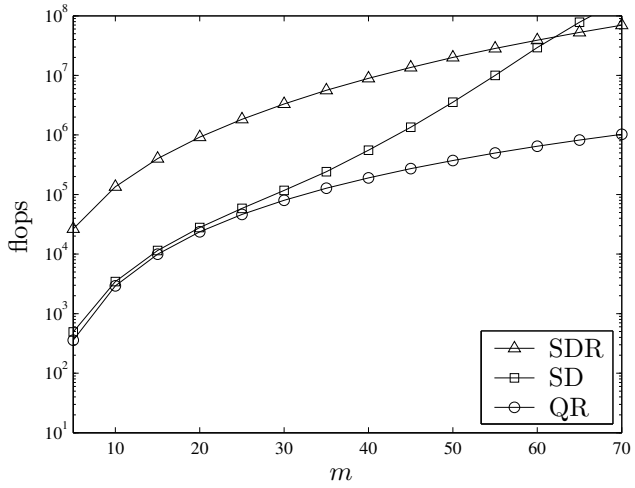


**Figure 5.4:** Average number of flops required by the SDR and SR algorithms as a function of the size, $m$. The average number of flops required by the QR factorization in the SD algorithms is included for reference.

where $\mathbf{s}$ is the vector of transmitted symbols. Thus, the probability of the search sphere being empty is below the target error probability of $10^{-2}$.

In the complexity simulations the number of floating point operations (flops) required by the algorithms where counted. By floating point operation additions, subtractions, multiplications, divisions, square roots, and floating point comparisons where considered. Since the majority of operations executed in the algorithms are either multiplications or additions there would be no significant change in the result if traditionally more computationally heavy operations such as square roots and divisions would have been considered to require several flops.

Figure 5.4 shows the average number of floating point operations for the sphere decoder and the semidefinite relaxation detector. As a reference the number of flops required by the QR factorization which precedes the enumeration stage of the sphere decoder is included. An interesting observation is that at the given SNR of 10dB the complexity of the sphere decoder is dominated by the complexity of the QR factorization for sizes up to about $m = 30$. Thus, if the algorithm is used to detect several

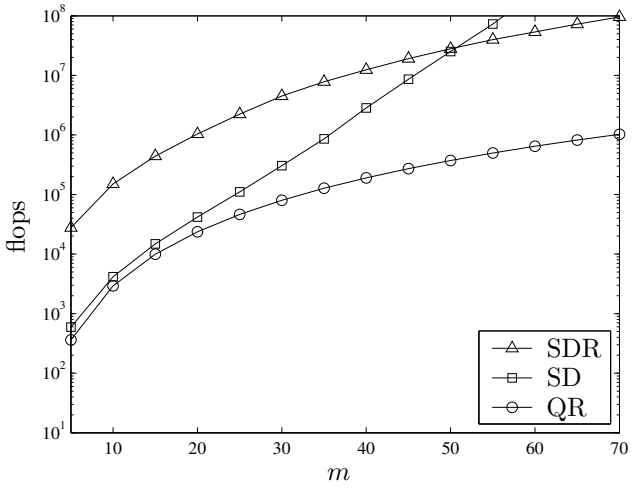


**Figure 5.5:** The first percentile of the number of flops required by the SDR and SR algorithms as a function of the size, $m$. This correspond to the worst case complexity required to ensure a BER of $10^{-2}$.

symbol vectors transmitted over the same channel the complexity of the algorithm may be significantly reduced in this range. For $m \geq 30$ the complexity of the algorithms is however dominated by the enumeration process. In this range the exponential complexity of the enumeration procedure can be seen in the figure. It is also noticeable that the semidefinite relaxation detector is of higher average complexity than the sphere decoder for sizes up to $m = 60$ which suggest that the semidefinite relaxation approach should be applied only to very large systems.

One feature of the semidefinite relaxation approach however is that its complexity is fairly independent of the particular problem instance. In Figure 5.5 the first percentile of the number of flops are shown, i.e. the constant $c$ such that

$$\mathrm{P}\left(C \geq c\right) = 10^{-2}$$

where $C$ is the number of flops given the channel $\mathbf{H}$ and the received symbols $\mathbf{y}$. Note that this is an upper bound on the complexity of the algorithms which is valid for 99 percent of the realizations. In an application where there is a hard limit on the complexity of the algorithms this is the number of operations which, at least, must be allowed for to

ensure the target error probability of $10^{-2}$. By comparing Figures 5.4 and 5.5 it can be seen that worst realizations of the sphere decoder are significantly above the average while for the semidefinite relaxation they are roughly the same. Note that this does not contradict the conclusion of (4.22) since what is established in (4.22) is that the asymptotic slope of the curves in Figures 5.4 and 5.5 must be the same. They may however differ from each other by some offset.

## 5.4 Summary

In this section the performance, both in terms of BER and computational complexity, of the SDR and the SD algorithms were numerically investigated. Most notable is that while it was proven by the analytical results of previous sections that the SDR algorithm must be of lower complexity SD algorithm for large $m$ there is a considerable range of $m$ for which the opposite is true. This suggests that from an implementation point of view the SDR algorithm is preferable only for large systems while the SD algorithm should be used for small to moderate size systems. Also, as can be seen by the BER investigations there is no noticeable difference between the algorithms in detection accuracy.

# Appendix 5.A Implementation Details

## 5.A.1 Semidefinite Relaxation

The semidefinite relaxation algorithms used in this chapter was implemented based on the pseudo code published in [TR01]. The pseudo code of [TR01] is in turn based on the algorithm published in [HRVW96]. The implementation of the SDR is a primal-dual interior point method which solves the KKT conditions of (3.8) iteratively. To obtain $\hat{\mathbf{s}}$ from the solution of (3.3) the randomized procedure outlined in [MDW$^+$02] was used with a square root factorization given by the Cholesky factorization and with $2m$ random trials. The pseudo code, `SPDSOLVE`, which given $\mathbf{L}$ outputs an $\mathbf{X}$ which approximately solves (3.3) is given in Table 5.1. Note however that the complexity calculations presented in this chapter include the operations required to form $\mathbf{L}$ and to perform the randomization procedure as well as the operations required by `SPDSOLVE`.

The computationally most costly part of the implementation of the SDR algorithm is that the inverse $\mathbf{Z}^{-1}$ in `SDPSOLVE` need to be explicitly computed. The inverse of this matrix is computed by the use of Algorithm 1.10 in [Ste98]. However since $\mathbf{Z}$ is known to be symmetric and positive definite the Cholesky factorization is conveniently used instead of the LU factorization. The verification required by Line 2 of `LINESEARCH` in Table 5.1 is done by the use of a, possible partial, Cholesky factorization. Further, whenever possible symmetry and positive definiteness of the matrices involved is utilized to reduce complexity in the implementation.

## 5.A.2 Sphere Decoder

The sphere decoder used in this chapter was implemented specifically for the binary constellation $\mathcal{S}^m = \{\pm 1\}^m$. As in [WMPF03] the QR-factorization published in [WBR$^+$01] was used to find a reordering of the symbols and to factor $\mathbf{H}$. The data dependent modification of the algorithms in [WBR$^+$01] considered in [WMPF03] was however not implemented.

In the enumeration stage the Schnorr-Euchnerr strategy [SE94] was employed together with an adaptively updated radius as outlined in Section 4.1. The pseudo code used to solve (4.1) given $\mathbf{R}$, $\mathbf{x}$, and an initial squared radius, $r^2$, `SDENUMERATION`, is given in Table 5.2. Note that the sum of the operations required by `SDENUMERATION` and the QR factorization are reported as the sphere decoder complexity.

SDPSOLVE($\mathbf{L}$)

$\mathbf{X} := \mathbf{I}$
$\mathbf{Z} := \mathbf{L}$
**for** $i = 1, \ldots, m+1$ **do**
  $[\mathbf{Z}]_{ii} := \sum_{j \neq i} |[\mathbf{Z}]_{ji}| + 1$, $[\mathbf{z}]_i := [\mathbf{L}]_{ii} - [\mathbf{Z}]_{ii}$
**end for**
**while** $(\mathrm{Tr}(\mathbf{XZ})/(m+1) < 10^{-5})$ **do**
  $\mu := \mathrm{Tr}(\mathbf{XZ})/(2(m+1))$
  $\Delta\mathbf{z} := (\mathbf{X} \circ \mathbf{Z}^{-1})^{-1}(\mu \ \mathrm{diag}(\mathbf{Z}^{-1}) - \mathbf{e})$
  $\Delta\hat{\mathbf{X}} := \mu\mathbf{Z}^{-1} - \mathbf{X} - \mathbf{X}\mathrm{Diag}(\mathbf{v})\mathbf{Z}^{-1}$
  $\Delta\mathbf{X} := (\Delta\hat{\mathbf{X}} + \Delta\hat{\mathbf{X}}^{\mathrm{T}})/2$
  $\Delta\mathbf{Z} := -\mathrm{Diag}(\Delta\mathbf{z})$
  $\alpha_p := \texttt{LINESEARCH}(\mathbf{X}, \Delta\mathbf{X})$
  $\mathbf{X} := \mathbf{X} + \alpha_p\Delta\mathbf{X}$
  $\alpha_d := \texttt{LINESEARCH}(\mathbf{Z}, \Delta\mathbf{Z})$
  $\mathbf{z} := \mathbf{z} + \alpha_d\Delta\mathbf{z}$
  $\mathbf{Z} := \mathbf{Z} + \alpha_d\Delta\mathbf{Z}$
**end while**

LINESEARCH($\mathbf{X}, \Delta\mathbf{X}$)

$\alpha := 1$
**while** $(\mathbf{X} + \alpha\Delta\mathbf{X} \succeq \mathbf{0})$ **do**
  $\alpha := 0.9\alpha$
**end while**

**Table 5.1:** Semidefinite program solver. Given a symmetric matrix, $\mathbf{L}$, the problem given in (3.3) is solved up to a tolerance of $10^{-5}$. The output is given in $\mathbf{X}$.

```
SDENUMERATION(R, x, r^2)
 1: i := m + 1, state := DOWN, r_i^2 := 0
 2: while (i ≤ m) or (state = DOWN) do
 3:   if (state = DOWN) then
 4:     i := i − 1
 5:     [z]_i := Σ_{j>i} [R]_ij [s̄]_j − [x]_i
 6:     [s̄]_i := sign([z]_i)
 7:     r_i^2 := ([R]_ii s̄_i − [z]_i)^2 + r_{i+1}^2
 8:     if (r_i^2 < r^2) then
 9:       if (i = 1) then
10:         r^2 := r_i^2, ŝ := s̄, state := UP
11:       end if
12:     else
13:       i := i + 1, state := DOWN
14:     end if
15:   else
16:     if ([s̄]_i := sign([z]_i)) then
17:       [s̄]_i := −[s̄]_i
18:       r_i^2 = ([R]_ii s̄_i − [z]_i)^2 + r_{i+1}^2
19:       if (r_i^2 < r^2) then
20:         state := DOWN
21:       end if
22:     else
23:       i := i + 1
24:     end if
25:   end if
26: end while
```

**Table 5.2:** Sphere decoder enumeration code. Given an upper triangular matrix, $\mathbf{R}$, with positive diagonal entries, a vector, $\mathbf{x}$, and a positive initial sphere radius, $r^2$, the code solves (4.1) under the condition that there is some $\hat{\mathbf{s}}$ which satisfies $\|\mathbf{x} - \mathbf{R}\mathbf{x}\| \leq r^2$. The output is given as $\hat{\mathbf{s}}$.

# Chapter 6

# Conclusions

In this thesis two algorithms for the solution, or approximate solution, of the ML detection problem in digital communications were investigated. In the case of the semidefinite relaxation it was previously known that the algorithm is of polynomial, $O(m^{3.5})$, complexity but suboptimal. Therefore, an investigation into for which problem realizations the semidefinite relaxation approach obtains the ML estimate was conducted. The conclusion was that if the noise is considered as a perturbation of the possible noise free constellation points at the receiver, the semidefinite relaxation algorithm is guaranteed to obtain the ML estimate if the perturbation is with certain bounds.

In the case of the sphere decoder it was previously known that the algorithm could attain the ML estimate. It is also well understood for which realizations the sphere decoder does not obtain the ML estimate when implemented suboptimally, i.e. with a finite initial search radius. However, in the case of the sphere decoder the questions about complexity are more difficult to answer. There are previously known upper bounds on the complexity of the algorithm but theses bounds are generally very loose, especially when considering the expected complexity of the algorithm. There are also exact expressions for the expected complexity of the algorithm for the case of the i.i.d. Rayleigh fading channel but these tend to be somewhat complicated. Also, from these expressions alone it is not obvious if the expected complexity is polynomial or exponential.

In this thesis it was shown that, if

1. the SNR experienced by any single symbol does not tend to infinity with $m$,

2. the probability that the search sphere is non-empty does not tend to zero as the size, $m$, of the problem is increased,

the expected complexity will tend to infinity as an exponential function. The rate at which the expected complexity for the sphere decoder tends to infinity was established for the i.i.d. Rayleigh fading channel by the use of tools from large deviations theory. This asymptotic analysis also, not surprisingly, showed that by increasing the SNR the exponential rate was decreased. This confirms previous observations that the complexity of the sphere decoder is reduced by an increased SNR. However, the asymptotic analysis of Section 4.3.1 gives a more precise meaning to this statement by quantifying how large the reduction is.

## 6.1 Topics for Future Work

While some questions have found their answers in this work there are still many issues not resolved. A few thoughts about some of these are given below.

### 6.1.1 Semidefinite Relaxation

- A problem with the analysis of Section 3.2 is that for many realizations, see Figure 5.3, the solution to the relaxed problem is not of rank one. In these cases a randomization procedure is used to obtain an approximation of the ML estimate. By comparing Figure 5.3 with Figures 5.1 and 5.2 it can be seen that the closeness to ML performance of the SDR indeed depends on this randomization procedure as the rank one solutions are not enough to ensure low error probability.

  Therefore, to explain the performance of the SDR approach the randomization procedure needs to be further investigated. To establish the diversity order of the SDR for the Rayleigh fading channel such randomizations will need to be taken into account. The former is especially interesting since numerical evidence suggests that it may be the case that the SDR achieves full diversity which would be quite remarkable if true.

### 6.1.2 Sphere Decoding

- As stated in Section 4.2.2 the exponential expected complexity results are not proven under the assumption that the symbols are reordered prior to detection. Recent investigations reveal that in the i.i.d. Rayleigh fading scenario the exponential expected complexity result still holds under arbitrary, data dependent, permutations of the symbols. Similar results can also be shown for other classes of channel matrices under restrictions on the possible permutation strategies.

  It would be interesting to further investigate for which channel distributions and ordering strategies the sphere decoder has exponential expected complexity.

- The asymptotic analysis of Section 4.3 does not allow adaptive updates of the search sphere radius during the search. It seems likely that for the high SNR scenarios, such updates will not substantially change the asymptotic expected complexity. However, how to establish such a conclusion in a stringent manner is at this point unclear.

# Bibliography


[AEVZ02] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger. Closest point search in lattices. *IEEE Transactions on Information Theory*, 48(8):2201–2214, August 2002.

[AHU74] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, 1974.

[ANJM02] M. Abdi, H. El Nahas, A. Jard, and E. Moulines. Semidefinite positive relaxation of the maximum-likelihood criterion applied to multiuser detection in a CDMA context. *IEEE Signal Processing Letters*, 9(6):165–167, June 2002.

[ASH03] H. Artes, D. Seethaler, and F. Hlawatsch. Efficient detection algorithms for mimo channels: a geometrical approach to approximate ML detection. *IEEE Transactions on Signal Processing*, 51(11):2808–2820, November 2003.

[BB03] L. Brunel and J. Boutros. Lattice decoding for joint detection in direct sequence CDMA systems. *IEEE Transactions on Information Theory*, 49(4):1030–1037, April 2003.

[BTT02] E. Biglieri, G. Taricco, and A. Tulino. How far away is infinity? using asymptotic analyses in multiple-antenna systems. *2002 IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications*, 1:1–6, 2002.

[DAML01] O. Damen, K. Abed-Meraim, and M. S. Lemdani. Further results on the sphere decoder. In *Proc. ISIT'01*, page 333, June 2001.

[DCB00] O. Damen, A. Chkeif, and J.-C. Belfiore. Lattice code decoder for space-time codes. *IEEE Communications Letters*, 4(5):161–163, May 2000.

[DGC03] M. O. Damen, H. El Gamal, and G. Caire. On maximum-likelihood detection and the search for the closest lattice point. *IEEE Transactions on Information Theory*, 49(10):2389–2401, October 2003.

[DHZ95] A. Duel-Hallen, J. Holtzman, and Z. Zvonar. Multiuser detection for CDMA systems. *IEEE Personal Comm.*, pages 46–58, April 1995.

[Due95] A. Duel-Hallen. A family of multiuser decision-feedback detectors for asynchronous code-division multiple-access channels. *IEEE Transactions on Communications*, 43(2/3/4):421–434, February/March/April 1995.

[Due99] A. Duel-Hallen. Decorrelating decision-feedback multiuser detector for synchronous code-division multiple-access channel. *IEEE Transactions on Communications*, 41(2):285–290, February 1999.

[Dur96] R. Durett. *Probability: Theory and Examples*. Duxbury Press, second edition, 1996.

[DZ98] A. Dembo and O. Zeitouni. *Large Deviations Techniques and Applications*. Springer-Verlag New York Inc., second edition, 1998.

[FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, April 1985.

[Gra02] A. Grant. Rayleigh fading multi-antenna channels. *EURASIP Journal on Applied Signal Processing*, (3):316 – 329, March 2002.

[HB03] B. M. Hochwald and S. Brink. Achieving near-capacity on a multiple-antenna channels. *IEEE Transactions on Communications*, 51(3):389–399, March 2003.

[HH02] B. Hassibi and B. M. Hochwald. High-rate codes that are linear in space and time. *IEEE Transactions on Information Theory*, 48(7):1804–1824, June 2002.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[HLP+04] F. Hasegawa, J. Luo, K.R. Pattipati, P. Willett, and D. Pham. Speed and accuracy comparison of techniques for multiuser detection in synchronous CDMA. *IEEE Transactions on Communications*, 54(4):540–545, April 2004.

[HRVW96] C. Helmberg, F. Rendl, R.J. Vanderbei, and H. Wolkowicz. An interior-point method for semidefinite programming. *SIAM Journal on Optimization*, 6:342–361, 1996.

[HV02] B. Hassibi and H. Vikalo. On the expected complexity of integer least-squares problems. In *Proc. IEEE ICASSP'02*, volume 2, pages 1497–1500, May 2002.

[HV03] B. Hassibi and H. Vikalo. Maximum-likelihood decoding and integer least-squares: The expected complexity. In J. Foschini and S. Verdú, editors, *Multiantenna Channels: Capacity, Coding and Signal Processing*. Amer. Math. Soc., 2003.

[JMO03] J. Jaldén, C. Martin, and B. Ottersten. Semidefinite programming for detection in linear systems – optimality conditions and space-time decoding. In *Proc. IEEE ICASSP'03*, April 2003.

[JO04a] J. Jaldén and B. Ottersten. An exponential lower bound on the expected complexity of sphere decoding. In *Proc. IEEE ICASSP'04*, May 2004.

[JO04b] J. Jaldén and B. Ottersten. On the expected complexity of sphere decoding in digital communications. To appear in *IEEE Transactions on Signal Processing*, 2004.

[JOM04] J. Jaldén, B. Ottersten, and W.-K. Ma. Reducing the average complexity of ML detection using semidefinite relaxation. Submitted to *IEEE ICASSP'05*, September 2004.

[LV89] R. Lupas and S. Verdú. Linear multiuser detectors for synchronous code-division multiple access channels. *IEEE Transactions on Information Theory*, 35(1):123–136, January 1989.

[MCDX04] W.-K. Ma, P.-C. Ching, T. N. Davidson, and X.-G. Xia. Blind maximum likelihood decoding of orthogonal space-time block codes: A semidefinite relaxation approach. In *Proc. IEEE ICASSP'04*, May 2004.

[MDW+02] W.-K. Ma, T. N. Davidson, K.M. Wong, Z.-Q Lou, and P.-C. Ching. Quasi-maximum-likelihood multiuser detection using semi-definite relaxation with application to synchronous CDMA. *IEEE Transactions on Signal Processing*, 50(4), April 2002.

[MDWC04] W.-K. Ma, T. N. Davidson, K.M. Wong, and P.-C. Ching. A block alternating likelihood maximization approach to multiuser detection. *IEEE Transactions on Signal Processing*, 52(9), September 2004.

[Mow92] W.H. Mow. Maximum likelihood sequence estimation from the lattice viewpoint. In *ICCS/ISITA '92*, volume 1, pages 127–131, November 1992.

[Mow94] W.H. Mow. Maximum likelihood sequence estimation from the lattice viewpoint. *IEEE Transactions on Information Theory*, 40(5):1591–1600, September 1994.

[Nes97] Y.E. Nesterov. Quality of semidefinite relaxation for non-convex quadratic optimization. Technical report, Technical Report, CORE, Universite Catholique de Louvain, Belgium, 1997.

[NW88] G. L. Nemhauser and L. A. Wolsey. *Integer and Combinatorial Optimization*. Wilie-Interscience, 1988.

[Poh81] M. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *ACM SIGSAM Bull.*, 66:181–191, 1981.

[Pro95] J. G. Proakis. *Digital Communications*. McGraw-Hill, third edition, 1995.

[Rud96] W. Rudin. *Principles of Mathematical Analysis*. McGraw-Hill International Editions, third edition, 1996.

[SE94] C.P. Schnorr and M. Euchnerr. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–191, 1994.

[SLW03] B. Steingrimsson, Z.-Q. Lou, and K.W. Wong. Soft quasi-maximum-likelihood detection for multiple-antenna wireless channels. *IEEE Transactions on Signal Processing*, 51(11), November 2003.

[Ste98] G. W. Stewart. *Matrix Algorithms. Volume 1: Basic Decompositions*. SIAM, 1998.

[SW95] A. Shwarts and A. Weiss. *Large Deviations for Performance Analysis*. Chapman and Hall, 1995.

[Tel99] I.E. Telatar. Capacity of multi-antenna gaussian channels. *European Trans. Telecomm*, 10(6):585–596, December 1999.

[TR01] P.H. Tan and L.K. Rasmussen. The application of semidefinite programming for detection in CDMA. *IEEE Journal on Selected Areas in Communications*, 19(8):1442–1449, August 2001.

[VA90] M. K. Varanasi and B. Aazhang. Multistage detection inasynchronous code-division multiple-access communications. *IEEE Transactions on Communications*, 38(4):509–690, April 1990.

[VA91] M. K. Varanasi and B. Aazhang. Near-optimum detection in synchronous code-division multiple-access systems. *IEEE Transactions on Communications*, 39(5):725–736, May 1991.

[Var95] M. K. Varanasi. Group detection for synchronous gaussian code-division multiple-access channels. *IEEE Transactions on Information Theory*, 41(4):1083–1096, July 1995.

[Var99] M. K. Varanasi. Decision feedback multiuser detection: a systematic approach. *IEEE Transactions on Information Theory*, 45(1):219–240, January 1999.

[VB93] E. Viterbo and E. Biglieri. A universal lattice decoder. In Proc. 14ème Colloque GRETSI, Juan-les-Pins, France, pages 611–614, September 1993.

[VB96] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38:49–95, 1996.

[VB99] E. Viterbo and J. Boutros. A universal lattice code decoder for fading channels. *IEEE Transactions on Information Theory*, 45(5):1639–1642, July 1999.

[Ver86] S. Verdú. Minimum probability of error for asynchronious gaussian multiple-access channels. *IEEE Transactions on Information Theory*, 32(10):85–96, January 1986.

[Ver89] S. Verdú. Computational complexity of multiuser detection. *Algorithmica*, 4:303–312, 1989.

[Ver93] S. Verdú. Multiuser detection. In H. V. Poor and J. B. Thomas, editors, *Advances in Statistical Signal Processing: Signal Detection*, pages 369–410. Greenwich CT: JAI Press, 1993.

[Ver98] S. Verdú. *Multiuser Detection*. Cambridge Univ. Press, Cambridge, U.K., 1998.

[VH02] H. Vikalo and B. Hassibi. Maximum-likelihood sequence detection of multiple antenna systems over dispersive channels via sphere decoding. *EURASIP Journal on Applied Signal Processing*, 2002(5):525–531, May 2002.

[WBR+01] D. Wubben, R. Bohnke, J. Rinas, V. Kuhn, and K.D. Kammeyer. Efficient algorithm for decoding layered space-time codes. *IEE Electronics Letters*, 37:1348–1350, October 2001.

[WLA03] X.M. Wang, W.S. Lu, and A. Antoniou. A near-optimal multiuser detector for DS-CDMA systems using semidefinite programming relaxation. *IEEE Transactions on Signal Processing*, 51(9):2446 – 2450, September 2003.

[WMPF03] A. Wiesel, X. Mestre, A. Pagés, and J. R. Fonollosa. Efficient implementation of sphere demodulation. In *Proc. SPAWC'03*, April 2003.

[WSV00] H. Wolkowicz, R. Saigal, and L. Vandenberghe, editors. *Handbook of Semidefinite Programming*. Kluwer Academic Publishers, 2000.

[XSR90] Z. Xie, R. T. Short, and C. K . Rushforth. A family of suboptiomum detectors for coherent multiuser communications. *IEEE Journal on Selected Areas in Communications*, 8(4):683–690, May 1990.