Lattices in MIMO Spatial Multiplexing: Detection and Geometry

Francisco A. T. B. N. Monteiro

(Fitzwilliam College)

Department of Engineering

University of Cambridge

May 2012

To Fotini

and

To my mother

Abstract

Multiple-input multiple-output (MIMO) spatial multiplexing (SM) allows unprecedented spectral efficiencies at the cost of high detection complexity due to the fact that the underlying detection problem is equivalent to the closest vector problem (CVP) in a lattice. Finding better algorithms to deal with the problem has been a central topic in the last decade of research in MIMO SM.

This work starts by introducing the most prominent detection techniques for MIMO, namely linear filtering, ordered successive interference cancellation (OSIC), lattice-reduction-aided, and the sphere decoding concept, along with their geometrical interpretation. The geometric relation between the primal and the dual-lattice is clarified, leading to the proposal of a pre-processing technique that allows a number of candidate solutions to be efficiently selected.

A sub-optimal quantisation-based technique that reduces the complexity associated with exhaustive search detection is presented.

Many of the detection algorithms for MIMO have roots in the fields of algorithmic number theory, theoretical computer science and applied mathematics. This work takes some of those tools originally defined for integer lattices and investigates their suitability for application to the rational lattices encountered in MIMO channels. Looking at lattices from a group theory perspective, it is shown that it is possible to approximate the typical lattices encountered in MIMO by a lattice having a trellis representation.

Finally, this dissertation presents an alternative technique to feedback channel state information to the transmitter that shifts some of the processing complexity from the receiver to the transmitter while also reducing the amount of data to be sent in the feedback link.

Declaration

This dissertation is submitted for the degree of Doctor of Philosophy. I hereby declare that this dissertation is not substantially the same as any that I have submitted for a degree or diploma or other qualification at any other university. I further state that no part of my dissertation has already been or is being concurrently submitted for any such degree, diploma or other qualification. I also declare that this dissertation is the result of my own work carried out at the University of Cambridge and includes nothing which is the of work done in collaboration, except where specified explicitly in the text and Acknowledgments. The length of this dissertation does not exceed 65,000 words and contains fewer than 150 figures, according to the limits stipulated by the Department of Engineering.

Francisco A. T. B. N. Monteiro
May 2012

Acknowledgements

I thank first of all Dr. Ian Wassell for his patience in supervising me and allowing me to attend the large number of lectures, talks, and courses in fields so much beyond the scope of my research topic, in the unique intellectual environment that Cambridge provides. Dr. Wassell's fast and reliable feedback to anything asked is unique. This thesis could not exist without his endless support and the confidence he showed in me.

I am thankful to both Prof. Alister Burr and Dr. Jossy Sayir for their insightful questions and comments during an intellectually stimulating and pleasant viva exam. Not only was this dissertation improved by their comments, but I was also happy in getting to know further links between current MIMO topics and earlier related problems.

My departmental affiliation in Cambridge was always a complicated affair; with an application to a group in the process of moving between departments, I ended up affiliated with both: the Department of Engineering and the Computer Laboratory. Given the scope of my research, this could not have proved more appropriate. Moreover, I was lucky in having full access to both departments, taking the best from the opportunities provided by both.

I thank Professor Frank Kschischang for the privilege of learning from his immense knowledge. I shall never forget the invitation to have Christmas Dinner at his house with his family when I was far from all. Also at Toronto, I thank Dr. Danilo Silva for his kindness and his example as a researcher.

In Cambridge I was lucky to have met a group of friends. I will never forget the intellectual brilliance of Dr. Karen Su, Dr. Ioannis Chatzigeorgiou for his example as

well-rounded academic and person and Dr. Bogdan Roman, whose theoretical and practical skills never cease to surprise me. I have no words to express how deeply thankful I am for the unshakeable confidence that Karen, Yannis and Bogdan showed in me, and how much I learnt from them.

I have also been privileged to learn from the academic example of Dr. Miguel Rodrigues and Dr. Ford Wong in the group.

I thank Dr. William Carson, Dr. Weisi Guo, Dr. Jaime Adeane, Ruoshui Liu and to Dr. Vaughan Wittorff for all the pleasant conversations we had over the years.

The friendship and human example of Dr. Yan Wu will be always remembered.

I thank Dr. Oded Regev for the long discussions on the orthogonal sublattice problem from the algorithmic perspective, and to Dr. Frédérique Oggier for discussing the same problem from the algebraic point of view. I also thank to Dr. Steven Galbraith for interesting conversations on the Babai algorithm and to Dr. Keith Matthews for discussions on the Hermite Normal Form.

I am thankful to all the libraries I have used in Cambridge: Engineering Department Library for supporting the borrowing from the British Library and for still allowing the pleasure of exploring the latest IEEE issues on paper; the Computer Laboratory Library, Fitzwilliam College Library, University Library, Betty and Gordon Moore Library, and Library of the Cambridge Philosophical Society, for the endless hours of discoveries and for having papers that "no other" has. In Toronto I am thankful to the libraries of the Electrical and Computer Engineering Department and the Mathematics Department, which also have "everything". The Portuguese B-on service was also important for accessing some of the papers.

My time in Cambridge was possible thanks to the scholarship from the Foundation for Science and Technology. The several months spent in Toronto were possible thanks to grants from the Gulbenkian Foundation, the Royal Academy of Engineering, the Cambridge Philosophical Society, the Digital Technology Group of The Computer Laboratory and Fitzwilliam College. Some other partial grants were obtained from the Instituto de Telecomunicações and the University Institute of Lisbon.

ACKNOWLEDGEMENTS

I am thankful to Professor Nick Kinsgbury and Dr. Albert Guillén i Fàbregas for their wise and timely advice on research paths and working methodologies.

I thank the students at Fitzwilliam College for their example, their talent, and for creating the most admirable of all environments to live in.

I am thankful for the teaching opportunity given to me by the University Institute of Lisbon.

No words are enough to thank Dr. Fotini Hadjittofi, now my wife, for all her support in the most difficult times. And I thank my mother Lourdes for all the support throughout all my life.

Contents

Abstract **v**

Declaration **vii**

Acknowledgements **ix**

Contents **xiii**

List of Figures **xvii**

List of Tables **xxiii**

Acronyms **xxv**

Symbols and Notation **xxix**

Chapter 1 – Introduction **1**

1.1 – MIMO in Context 1

1.1.1 – From Shannon to Codes on Graphs 1

1.1.2 – The First Appearance of Lattices: Coding for The Band-limited Channel 4

1.1.3 – The Advent of MIMO 5

1.1.4 – MIMO in Wireless Standards 7

1.2 – The Different Faces of MIMO 8

1.2.1 – Diversity and Multiplexing 9

1.2.2 – Space-time Codes (STC) 12

1.2.3 – Spatial Multiplexing (SM) 13

1.2.4 – Spatial Diversity Versus Spatial Multiplexing 17

1.2.5 – Multi-user MIMO 17

1.2.6 – Single-user Closed loop (Water-filling) 18

1.2.7 – Beamforming 19

1.2.8 – Channel Feedback 19
1.3 – Motivation and Scope 21
1.3.1 – Limitations of Scope 23
1.4 – Publications 23
1.5 – Dissertation Outline 23
Chapter 2 – Fundamentals on Lattices and Spatial Multiplexing 25
2.1 – Lattices 25
2.1.1 – Context 26
2.1.2 – Basic Definitions 27
2.1.3 – The Dual Lattice 34
2.2 – MIMO Spatial Multiplexing 38
2.2.1 – System Model 38
2.2.2 – The Real Equivalent Model 43
2.2.3 – Capacity with CSIR 44
2.3 – Detection in MIMO SM 47
2.3.1 – The Complexity of Optimal Detection 48
2.4 – Summary 51
Chapter 3 – Geometry and Detection in Spatial Multiplexing 53
3.1 – Linear Receivers 54
3.1.1 – Zero-forcing Detection 55
3.1.2 – The Geometry of ZF Detection 58
3.1.3 – Algebraic Analysis of ZF 60
3.1.4 – Minimum Mean Squared Error Detection 61
3.1.5 – Projection Matrices 66
3.2 – Ordered Successive Interference Cancellation 68
3.2.1 – The Geometry of Optimal Ordering 68
3.3 – Gram-Schmidt Orthogonalisation and QR Decomposition 75
3.4 – Lattice-Reduction-Aided Detection 77
3.5 – Sphere Decoding 82

3.6 – Dual-Lattice-Aided Detection 86
3.6.1 – Successive Minima in the Dual Lattice 86
3.6.2 – Projections Onto Hyperplanes 87
3.6.3 – List of Candidate Solutions 88
3.7 – Performance Comparison 90
3.8 – Summary 95

Chapter 4 — Exhaustive Search in Quantised Spaces 97

4.1 – Quantised Spaces 98
4.2 – Quantisation Error 99
4.2.1 – Uncorrelated Noise and Uncorrelated Data 100
4.2.2 – Saturation Does not Impair Detection 100
4.2.3 – Uniform Error Per Component 101
4.2.4 – Equal Saturation in the Dimensions (hypercube) 102
4.3 – The Look-Up Table Technique 103
4.4 – Simulation Results 104
4.5 – Summary 109

Chapter 5 — Alternative Representations of Lattices 111

5.1 – The Hermit Normal Form 112
5.2 – Representation by a Modular Equation 115
5.3 – Summary 120

Chapter 6 — Focusing Onto Orthogonal Quotient Groups 121

6.1 – Lattices with a Trellis Representation 121
6.2 – Focusing Onto Lattice Sets 123
6.3 – The $\mathcal{L}_R$ Family of Lattices 125
6.4 – Lattices with Orthogonal Sublattices 129
6.4.1 – The Quasi Orthogonal Sublattice Problem 129
6.4.2 – Properties of the Generator Matrix 132
6.4.3 – Geometrical Interpretation: Distortion vs Number of Cosets 133

6.4.4 – Lattice Construction Algorithm 136
6.5 – Number of Cosets 139
6.6 – Performance Comparison 144
6.6.1 – 2×2 Antennas 145
6.6.2 – 3×3 Antennas 147
6.6.3 – 4×4 Antennas 148
6.6.4 – 6×6 Antennas 150
6.7 – Discussion of the Results 150
6.8 – Focusing Onto Fixed Lattices in $\mathcal{L}_R$ 152
6.9 – Summary 154
Chapter 7 — Closed Loop Spatial Multiplexing 155
7.1 – Feedback in MIMO 155
7.2 – The Matrix Conversion Method 156
7.3 – Closed Loop Technique 158
7.4 – Assessment of the Approximation 164
7.5 – Summary 165
Chapter 8 — Conclusions 167
8.1 – Research Contributions 167
8.2 – Further Work 169
8.2.1 – Randomised Projections 170
8.2.2 – The Orthogonal Sublattice Problem 171
8.2.3 – The Lattice Distinguishing Problem 171
8.2.4 – Trellis Construction Methods 172
8.2.5 – Interference Alignment over Lattices 173
8.2.6 – Physical Layer Network Coding 173
Appendix A – Determinant of a Triangular Matrix 175
Appendix B – Lattice Geometry Tool 177
References 179

List of Figures

1.1 Wireless MIMO link (single-user setup). 8

1.2 Single-user MIMO with channel state information at the receiver and at the transmitter (either full information or the distribution). 20

2.1 A lattice in $\mathbb{R}^2$ and the fundamental region associated with a particular basis. 29

2.2 The elementary operation that skews the fundamental region of a lattice preserves the determinant. The two shaded areas are the same. 33

2.3 A primal lattice in n dimensions as the union of translates of a sublattice and these translates lie on $(n-1)$-dimensional hyperplanes. 36

2.4 Identification of the hyperplanes in the primal lattice (on the left side) associated with a certain point in the dual lattice (on the right side). 37

2.5 Spatial multiplexing with real inputs. $\mathbb{Z}^n$ is transmitted and then skewed by the effect of the channel. 39

2.6 The closest vector problem in one, two and three dimensions, given an off-lattice target point. 48

2.7 Complexity classes. 49

3.1 Zero-forcing receiver. 56

3.2 Geometric interpretation of ZF filtering in a signal space. 57

3.3 Decision regions associated with the two different bases of the same lattice. 59

3.4 Orthogonality principle: the expected error is made orthogonal between the receive vector and the space where the best solution is searched. 62
3.5 MMSE receiver. 64
3.6 Geometry of the SNR relation factor in (3.25). Includes the Voronoi regions and the ZF decision regions of the lattice $\Lambda(\mathbf{H}_2)$, as given in (3.7). 68
3.7 The nearest plane algorithm with sorting. Choosing the j^{th} generator vector that maximises the distance between parallel hyperplanes. The lattice is the union of such translates. 72
3.8 Errors events in SIC. Plane 1 is selected because it is the closest plane, however, the closest lattice point lies in plane 2. The SIC decision region for the origin is shown. 73
3.9 A reduced basis (green) and a skewed basis (red) for the same lattice. 78
3.10 MIMO detection with lattice-reduction pre-processing. 78
3.11 The Gauss' algorithm (i.e., LLL in 2D). 80
3.12 Receiver based on sphere decoding. 82
3.13 Tree exploration of a tree with 3 layers, considering a 4-PAM alphabet. 83
3.14 Points inside a sphere centred at the origin of the dual lattice and containing $L = 7$ USM (denoted by dots with circles around). 87
3.15 Dual-lattice-aided generation of candidate solutions considering $\nu_{\max}$=1 and considering L=3 families of hyperplanes: the two families in Figure 3.14 and also the family associated with the dual vector $h_2^{(D)} = (1,3)$ 89
3.16 Detection in n=4 real dimensions (2×2 antennas) with 64-QAM. 92
3.17 Detection in n=6 real dimensions (3×3 antennas) with 64-QAM. 92
3.18 Detection in n=8 real dimensions (4×4 antennas) with 64-QAM. 93
3.19 Detection in n=12 real dimensions (6×6 antennas) with 64-QAM. 93

4.1 Quantiser with $\Theta = 8$ levels ($b = 3$ bits) in each dimension normalising the input to y_{sat} 99

4.2 The two components of the *complex* lattice of a 2×2 system with QPSK symbols ($M^{N_T} = 16$).....101

4.3 Quantisation error for the squared Euclidean distance as a function of the number of quantisation bits, b , obtained by simulation.....102

4.4 Additional bits required to compensate the loss associated with more dimensions in the lattice.....103

4.5 Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 2×2 system using QPSK modulation.....105

4.6 Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 3×3 system using QPSK modulation.....106

4.7 Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 4×4 system using QPSK modulation.....106

4.8 Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 2×2 system using 16-QAM.....107

6.1 The set of lattices and the focusing operator. A received lattice Λ can be focused onto the nearest member of $\mathcal{L}_R$ or onto $\mathbb{Z}^n$ 124

6.2 Detection on an approximated trellis representation. 124

6.3 A rectangular sub-lattice in a random lattice and the trellis representation of the lattice.....126

6.4 The rectangular quotient group of the A_2 lattice, exhibiting two cosets. 127

6.5 One of the possible trellises of the Schläfli lattice, D_4 (with 6 paths).....128

6.6 One of the possible trellises of the Gosset lattice, E_8 (with 16 paths). 128

6.7 A lattice given by $(\mathbf{h}_1, \mathbf{h}_2)$ with a rectangular sublattice (with its points "*" inside squares) and a near lattice generated by $(\tilde{\mathbf{h}}_1, \tilde{\mathbf{h}}_2)$, obtained from $(\mathbf{h}_1, \mathbf{h}_2)$ rotated by 5 degrees anticlockwise (depicted by "*"). 131

6.8 Approximation versus number of cosets: the dilemma of the approximation in the dual lattice (example in a 3D space). 135

6.9 Evolution of the number of cosets and Frobenius distance in Algorithm 3.1 for a n=4 dimensional random lattice as the error tolerance increases. 138

6.10 Evolution of the number of cosets and Frobenius distance in Algorithm 3.1 for a n=8 dimensional random lattice as the error tolerance increases. 138

6.11 Probability density function of the number of cosets in n=4 real dimensions (2×2 configurations), limiting to Γ=50. 141

6.12 Probability density function of the number of cosets in n=4 real dimensions (2×2 configurations), limiting to Γ=100. 142

6.13 Probability density function of the number of cosets in n=6 real dimensions (3×3 configurations), limiting to Γ=200. 142

6.14 Probability density function of the number of cosets in n=8 real dimensions (4×4 configurations), limiting to Γ=100. 143

6.15 Probability density function of the number of cosets in n=8 real dimensions (4×4 configurations), limiting to Γ=500. 143

6.16 Probability density function of the number of cosets in n=12 real dimensions (6×6 configurations) , limiting to Γ=10,000..... 144

6.17 Detection in n=4 real dimensions (2×2 antennas) with QPSK. 145

6.18 Detection in n=4 real dimensions (2×2 antennas) with 16-QAM. 146

6.19 Detection in n=4 real dimensions (2×2 antennas) with 64-QAM. 146

6.20 Detection in n=6 real dimensions (3×3 antennas) with QPSK. 147

6.21 Detection in n=6 real dimensions (3×3 antennas) with 16-QAM. 147

6.22 Detection in n=6 real dimensions (3×3 antennas) with 64-QAM. 148

6.23 Detection in n=8 real dimensions (4×4 antennas) with QPSK. 148

6.24 Detection in n=8 real dimensions (4×4 antennas) with 16-QAM. 149

6.25 Detection in n=8 real dimensions (4×4 antennas) with 64-QAM. 149

6.26 Detection in n=12 real dimensions (6×6 antennas) with 64-QAM.....150

6.27 Slice of dimensions 3 and 4 of a 4-dimensional lattice overlapped with the nearest synthetic lattice found (with Φ=495 cosets). Both lattices are depicted together with their Voronoi regions. 152

6.28 Comparison of the ZF decision region with the one corresponding to a focusing onto A_2. ML (thin blue), Zero forcing (black) and image of the hexagonal fundamental region of A_2 153

7.1 Proposed closed loop transmission scheme. 162

7.2 Processing at the transmitter. 162

7.3 Processing at the receiver. 162

7.4 Probability distribution of the squared Frobenius norm of the error matrix for $\tilde{\mathbf{G}}$ (or $\tilde{\mathbf{G}}'$). 165

List of Tables

1.1 Configurations depending in the input and output. 9

1.2 Different names of analogous techniques. 16

2.1 Symbol energy for the used modulations. 40

3.1 Number of operations involved in solving $\mathbf{y} = \mathbf{Hx}$ by several methods based on channel inversion (with a square $\mathbf{H}$) 58

3.2 Number of candidates in DLA. 90

7.1 Comparison of the complexities of the schemes 164

Acronyms

3GPP	3rd generation partnership project
ASK	Amplitude Shift Keying
AWGN	Additive while Gaussian noise
BCJR	Bahl-Cocke-Jelinek-Raviv (algorithm)
BER	Bit error rate
BC	Broadcast channel
BS	Base station
CLLL	Complex-LLL
CS	Compressed sampling
CSIR	Channel state information at the receiver
CSIT	Channel state information at the transmitter
CVP	Closest vector problem
D-BLAST	Diagonal Bell Labs layered space-time
DL	Downlink
DLA	Dual-lattice-aided
FCSD	Fixed Complexity sphere decoding
FDMA	Frequency division multiple access
GS	Gram-Schmidt
HNF	Hermite Normal Form
i.i.d.	Independent and identically distributed
IA	Interference alignment
ISI	Inter-symbol interference

LAST	Lattice space-time
LDP	Lattice distinguishing problem
LLL	Lenstra Lenstra Lovász
LR	Lattice reduction
LRA	Lattice-reduction-aided
LTE	Long term evolution
MAC	Multiple access channel
MAP	Maximum *a posteriori* probability
MCR	Maximum ratio combining
MIMO	Multiple input multiple output
MISO	Multiple input single output
ML	Maximum likelihood
MLD	Maximum likelihood detection
MLQS	Maximum likelihood in a quantised space
MLSD	Maximum likelihood sequence detection
MMSE	Minimum mean squared error
MPCP	Matching point clouds problem
M-QAM	(M-ary) quadrature amplitude modulation
MUD	Multiuser detection
NP	Non-deterministic polynomial time
OFDM	Orthogonal frequency division multiplexing
OSTBC	Space-time orthogonal block codes
PAM	Pulse amplitude modulation
pdf	Probability density function
PLNC	Physical layer network coding
PSK	Phase shift keying
QPSK	Quadrature PSK
Rx	Receiver
SD	Sphere decoding

SED	Squared Euclidian distance
SER	Symbol error rate
SIC	Successive interference cancelation
SIMO	Single input multiple output
SISO	Single input single output
SM	Spatial multiplexing
SNR	Signal to noise ratio
STC	Space-time codes
STTC	Space-time trellis codes
SVD	Singular value decomposition
TCM	Trellis coded modulation
TDMA	Time division multiple access
Tx	Transmitter
UB	Upper bound
UL	Uplink
UMTS	Universal mobile telecommunications system
USM	Unique successive minima
u.t.	Upper triangular
VA	Viterbi algorithm
VLSI	Very large scale integration
V-BLAST	Vertical Bell Labs layered space-time
WiMAX	Worldwide interoperability for microwave access
ZF	Zero-forcing
ZMSW	Zero-mean spatially white

Symbols and Notation

Latin alphabet

$\mathcal{A}$	Symbol alphabet (real PAM signals)
$\mathcal{A}_c$	Symbol alphabet (complex constellation)
a	Multiple of column that is added to another column
E_s	Energy of a complex symbol
c_i	Quantisation level
$\mathcal{C}$	Set of candidates in DLA
C	Spherical region associated with the distance to the saturation surface
$\mathbf{D}$	Diagonal matrix
$\tilde{\mathbf{D}}$	Diagonal matrix obtained by the truncated Lenstra algorithm
$\mathbf{D}_{eq}$	Equivalent diagonal matrix resulting from the product of two
D	Distance between parallel hyperplanes
d	Diversity order
d_{jj}	Diagonal elements in $\mathbf{D}$
$\tilde{d}_{jj}$	Truncated expantion of d_{jj}
$\mathbf{e}_z$	Vector $\mathbf{z}$ normalised to norm one
$\mathcal{F}$	Focusing linear transformation
$\mathbf{G}$	Gram matrix
$\tilde{\mathbf{G}}$	Gram matrix resulting from the truncated Lenstra algorithm
$\mathbf{G}_{1/2}$	Upper or triangular part of a Gram matrix
$\mathbf{H}_c$	Channel matrix and lattice generating matrix (complex entries)

$\mathbf{H}$	Channel matrix and lattice generating matrix (real entries)
$\widehat{\mathbf{H}}$	Generating matrix for an equivalent lattice
$\mathbf{H}_{\bar{j}}$	Matrix obtained from $\mathbf{H}$ by suppressing its j^{th} column
$\overline{\mathbf{H}}$	GS orthogonalised basis
$\tilde{\mathbf{H}}$	Approximated basis in $\mathcal{L}_R$
$\mathbf{H}^{(D)}$	Lattice generating matrix (real) of the dual lattice
$\tilde{\mathbf{H}}^{(D)}$	Approximated dual matrix in $\mathcal{L}_R$
$\mathbf{H}_{\text{HNF}}$	HNF of $\mathbf{H}$
$\tilde{\mathbf{H}}_{\text{HNF}}$	Perturbed HNF of $\mathbf{H}$ with a 1-cycle stucture
h_{ij}	Real channel fading coefficient
$h_{c,ij}$	Complex channel fading coefficient
$\overline{\mathbf{h}}_i$	Orthogonalised Gram-Schmidt vector
$\mathbf{I}_n$	Identity matrix $n \times n$ (the dimension is often omitted)
K	Number of branches expanded at each layer in a K-best decoder
$\mathcal{L}_R$	Family of lattices with a trellis representation
$\mathbf{L}$	Lower triangular matrix
$\mathbf{L}_u$	Non-zero off-diagonal elements in $\mathbf{L}$
L	Number of USM
$\mathcal{M}$	The set of all possible complex lattices
$M_{i,j}$	Minors of a matrix
$\mathbf{M}$	Unimodular matrix
M	Number of complex symbols in a QAM constellation
N_0	Unilateral noise spectral density
N_R	Number of receive antennas
N_T	Number of transmit antennas
n	Number of dimensions of a real lattice
$\mathbf{n}_q$	Quantisation noise vector
n	Additive noise vector

$OD(\mathbf{H})$	Orthogonality defect of basis $\mathbf{H}$
P	Signal power
$\mathcal{P}(\nu)$	Family of hyperplanes, each hyperplane defined by an integer ν
$\mathbf{P_H}$	Projection matrix onto the span of $\mathbf{H}$
$\mathbf{P_{H^\perp}}$	Projection matrix onto the space orthogonal to the span of $\mathbf{H}$
P_{W_i}	Projection lattice onto W_i
P_{V_i}	Projection lattice onto V_i
p	Exponent in a BER of the form 10^{-p}
p_{ij}	Numerators of $\tilde{\mathbf{H}}^{(D)}$
q	Quantisation step
q_{ij}	Denominators of $\tilde{\mathbf{H}}^{(D)}$
$\mathbf{R}_n$	Auto-correlation of the noise
$\mathbf{R}_x$	Auto-correlation of the transmit data
r_i	Length of the fundamental region of Λ_R in dimension i
r_{ij}	Element in the u.t. matrix $\mathbf{R}$ of the QR decomposition
s_i	Singular values of $\mathbf{H}$
T_s	Time duration of a complex symbol
t	Number of cycles of a lattice t
$\mathbf{U}$	Unitary matrix
$\mathbf{V}$	Unitary matrix
$\mathbf{v}_i$	Vector orthogonal to a family of hyperplanes
$\mathbf{W}$	Receive filter (focusing) for a certain detection technique
V_i	Subspace constituted by dimensions from 1 to i
W_i	One-dimensional space collinear with the i^{th} generator of Λ_R
$\mathbf{x}$	Transmitted vector (real elements)
$\hat{\mathbf{x}}$	Detected vector with a certain detection technique
$\mathbf{x}_c$	Transmitted vector (complex elements)

$\overline{\mathbf{x}}$	Detected vector of transmitted symbols
$\mathbf{x}_W$	Vector of symbols before quantization for detection
$\tilde{y}_i$	Quantised component of $\mathbf{y}$
$\mathbf{y}$	Received vector (real elements)
$\mathbf{y}^{(l)}$	Points in the finite lattice of interest
$\mathbf{y}_c$	Received vector (complex elements)
$\mathbf{y}_{sat}$	Clipping value for all quantised components

Greek alphabet

α	Complexity factor in SD
Γ	Maximum admissible number of cosets
Δ	Small real number
δ	Error tolerance incremental step
ε	Small real number
Φ	Number of cosets
Λ	Primal lattice
Λ'	Sublattice
$\Lambda^{(D)}$	Dual lattice
Λ_R	Rectangular sublattice
λ_i	i^{th} eigenvalue of $\mathbf{H}$
$\mu_{j,k}$	Gram-Schmidt coefficient
ν	Integer defining one of the parallel hyperplanes
Π	Permutation for OSIC
Θ	Number of quantisation levels
ρ	SNR
ρ_a	SNR normalised to the number of transmit antennas
Σ	diagonal matrix with singular values

σ	Linear transformation to approximate a lattice by a cycle lattice
σ_n^2	Real noise variance
σ_x^2	Variance (or power) of the (complex) constellation symbols
Ω	Index of a normalised projection of the target $\mathbf{y}$ onto $\mathbf{v}$.
Ξ	Pre-stored components
ξ	Sphere radius

Notation

$\mathbf{0}$	Column vector of zeros
$\mathbf{1}$	Column vector of ones
$\lfloor x \rfloor$	rounding to the closest integer that is not greater than x
$\lceil x \rceil$	rounding to the closest integer that is not smaller than x
$\langle \mathbf{a}, \mathbf{b} \rangle$	Inner product between vectors $\mathbf{a}$ and $\mathbf{b}$
$\left\|\mathbf{H}\right\|_F$	Frobenius norm of matrix $\mathbf{H}$
$\mathbb{C}^n$	n-dimensional complex space
$\mathbb{R}^n$	n-dimensional real space
$\mathbb{Z}^n$	n-dimensional vectors with integer coordinates
$\det(\mathbf{H})$	Determinant of $\mathbf{H}$
$\text{diag}(\mathbf{P})$	Diagonal of matrix $\mathbf{P}$
$E\{x\}$	Expected value of x
$(\cdot)^H$	Hermitian operator (conjugation fallowed by transposition or vice-verse)
$(\cdot)^T$	Transposition
$\mathcal{O}(\cdot)$	"Big O" notation for the upper bound on complexity
$\text{Proj}_{\mathbf{H}}(\mathbf{a})$	Projection of $\mathbf{a}$ onto the space spanned by $\mathbf{H}$
$\text{Proj}_{\mathbf{H}^\perp}(\mathbf{a})$	Projection of $\mathbf{a}$ onto the space orthogonal the one spanned by $\mathbf{H}$
$Q_{\mathcal{A}}()$	Quantisation to the alphabet $\mathcal{A}$
$Q_{\mathbb{Z}}()$	Quantisation to integers

$Q_\theta()$	Quantisation to a domain with Θ levels
$\mathrm{Vol}\big(\Lambda\big)$	Volume of lattice Λ

Chapter 1 – Introduction

"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point."
Claude Shannon, 1948. In [1], 2nd paragraph.

1.1 – MIMO in Context

The last ten years of research in communication theory have been characterised by extensive research in multiple-input multiple-output systems (MIMO). Reaching what Shannon's mathematical theory of communication found to be possible for the white additive Gaussian channel was a research task spanning 45 years (from 1948 to 1993). On the other hand, the intense research on MIMO since in the late 1990's achieved theoretical breakthroughs on MIMO rather more quickly. In fact, in the last ten years, the research community was able to put in practice many of the predictions of the theory, discover several nuances in the MIMO framework and develop them. Indeed, MIMO is making possible a new generation of wireless communication standards, both indoors and mobile.

1.1.1 – From Shannon to Codes on Graphs

When Claude Shannon presented his Master thesis in 1937 [2] showing that electronics could resolve logical (Boolean) statements, this was thought by many as something of little practical value. Shannon's research on the transmission of discrete symbols was much ahead of the electronics of the time. Similarly, Alec Reeves' pulse

coded modulation, presented in the same year, also had to wait a couple of decades for widespread implementation, after the invention of the transistor in 1947. Some criticism of the *digital concept* linked the *new* ideas to the then century-old telegraphy. Indeed, Nyquist's papers in the 1920's on sampled signals were linked to telegraphy in their titles. The advantages of digital communications would have to justify the need for more complicated circuitry than that required by analogue transmission [3]. Nevertheless, those advantages were very clear in Shannon's 1948 paper: error-free binary transmission can be achieved despite the presence of additive white Gaussian noise (AWGN) added to the signal and despite a finite bandwidth, as long as the transmission rate, R, is kept below the *capacity* of the channel. The advantage that a signal could now be detected and regenerated is an immediate consequence of this.

Shannon's proof of the capacity of a channel is based on an argument involving the average performance of the ensemble of all possible codes; if the performance of the average *is* known, then there must be *at least one* code that performs better than the average of all of them (as it is trivial to show that many codes lead to worse performance than the average). Shannon's clever proof was non-constructive and thus does not say anything about the code that would achieve the predicted capacity. This opened a race that included mathematicians, engineers, and computer scientists, looking for a family of capacity achieving codes for the AWGN channel. Most of the research was based on algebraic constructions of *block codes* that would maximise the minimum distance between codewords while keeping some structure that would limit the complexity of the decoder. Convolutional codes were developed alongside, falling into the so called category of *probabilistic codes*, differing from algebraic coding by maximizing the *average* distance between codewords, an idea that may be said to be closer to the initial ideas in Shannon's work. Most coding applications favoured the use of convolutional codes instead of algebraic block codes, mostly because of the efficiency conveyed by the Viterbi algorithm (for sequence detection on a trellis), an algorithm which became pervasive in several applications [4]. Forney [5], and later Kschischang and Sorokine [6] eventually showed that block codes (also called *group codes*, as they

are best understood in the context of group theory in mathematics) could also be described by trellises and thus that they too can be decoded by means of the Viterbi algorithm. In fact, the famous 1974 paper presenting the Bahl-Cocke-Jelinek-Raviv (BCJR) algorithm [7] already contained (on p. 287) the tools to construct a trellis of a block code (using what later became known as *construction A* [5]). Biglieri gives a concise description of the construction of the minimal trellis of a block code in [8] and comprehensive analyses exist by Shu Lin [9] and Honary [10]).

It was only in 1993, with the discovery of turbo-codes, and later in 1995 with the re-discovery of the Gallager codes (or LDPCs - low density parity check codes) that the quest was over (a thorough historical account by two of the most preeminent coding theorists can be found in [11], along with significant technical details; a concise history was given by the author of the thesis in [12]). Ironically, the solutions were the outcome of very different approaches to code design. Turbo-codes applied ideas of feedback coming from electronics (in this case information feedback) and LDPCs are an instance of concepts matured in the discipline of machine learning. It is today well known that both turbo-codes and LDPCs, along with *repeat-accumulate* (RA) codes, can be described under the single umbrella of *codes on graphs* [13]. Their decoding uses *belief propagation* in factor graphs [14], also known as *Bayesian networks* [15]. These ideas are known in communications as *iterative decoding* [16] (note that these names vary throughout the research communities).

The aforementioned codes are designed for the binary symmetric channel, as initially modelled by Shannon, and they all have a certain code rate. In the early 2000s a different family of codes emerged, said to be *rateless codes*, as one cannot define a fixed code rate for them. They have been discovered in the form of *fountain codes* or *raptor codes* and are specially designed for the *erasure channel* [1]. They are also all defined and decoded as codes on graphs [15] (ch.6). It is worth mentioning that for the *deletion*

[1] In the erasure channel the receiver is unable to decide or does not receive some of the data symbols but is aware of that loss and where and how many symbols were lost.

channel [2] little is known. Its capacity is still an open problem and, to the best of our knowledge, no practical schemes exist to cope with the deletion channel.

1.1.2 – The First Appearance of Lattices: Coding for The Band-limited Channel

In bandwidth-limited channels, binary antipodal signalling is not a solution to the communication problem, whatever the channel code that is used. The capacity of a channel depends on the *code rate* of the channel code (i.e., a real number in [0 1]). When bandwidth is not a limitation, one can tolerate reducing the rate of the code. Such an approach is useful in space applications, where the bandwidth is less of a problem than the power constraints associated with receiving bits from a distant small probe. In most other contexts, as spectrum is both limited and expensive, one needs to resort to multi-level modulations, such as quadrature amplitude modulation (QAM). Coding for these channels historically started with the design of lattice codes, characterised by the lattice they use to define the code words in a multidimensional space and a *shaping region* that limits the lattice, defining a finite point constellation [17], [18]. Selecting the lattice is a problem rather close to the seminal ideas in Shannon's work, as it amounts to a multi-dimensional sphere packing problem, as mentioned previously [19] [20]. To minimize the average power of the code words, the shaping regions should be a hyper-sphere, which causes some technical problems while decoding. It should be noted that when changing from a hyper-cubic shaping region to an optimal one there is an associated coding gain of 1.53 dB (the sometimes famous $\pi e / 6$ gain in linear units, also well known in quantization problems), which can *only* be obtained by a proper shaping[21]. However, achieving this gain increases the complexity of the decoder and the selection of a particular lattice is a difficult task in itself [22].

[2] In the deletion channel the receiver does not receive some of the data symbols, but the next ones are shifted filling that time gap and the receiver is unaware of the loss and does not know where and how many symbols are missing. Only some bounds to the capacity are know, mostly after Mitzenmacher's work at Harvard University.

Ungerboeck's trellis-coded modulation (TCM) [23] was the breakthrough that became the most popular technique for the band-limited channel in the 1980s, perhaps because decoding is based on the Viterbi algorithm, which was well understood by practicing engineers since its discovery predated TCM.

Lattice-based channel coding also proved important for the Rayleigh fading channel in the 1990's [24]. Authors such as Boutros, Viterbo and Belfiori later remained very active in the design of space-time codes for MIMO and seminal work by the first two authors for decoding of lattice codes later proved extremely important for optimum detection in MIMO.

Eventually, lattice structures were also proven to be able to reach the capacity of the AWGN channel in seminal work by Erez and Zamir [25]. More recently, new capacity achieving codes for the AWGN channel put together ideas from LDPCs and lattices using a sparse generator for the dual lattice[3] [26]

1.1.3 – The Advent of MIMO

The surprise of the discovery of the first capacity-achieving codes could have been seen as the end of communication theory by around 1995. Yet, at the same time new ideas by Foschini made room for unprecedented channel capacities for the wireless channel with multipath fading arising from rich scattering environments. Suddenly, Shannon's famous formula was no longer the limit [27] as multipath could be seen not as an impediment but as enabling multiple parallel channels. In 1996 Foschini at Bell Labs proposed a concept for parallel transmission utilising *layers* [28] where several antennas are used at both the transmitter and the receiver. The idea of using multiple antennas for more than just *maximal ratio combining* (MRC is a spatial version of the matched filter and was well known and used in several systems) was not entirely new, but until then no scheme had been considered simple enough for any practical use. Paulraj and Kailath with a USA patent granted in 1994, which made use of spatial multiplexing (SM) for increased throughput in wireless digital video, are by many

[3] A detailed description of dual lattices will be given in Chapter 2.

credited as the pioneers in MIMO. The 1999 landmark paper by Telatar [29][4] showed that the capacity increases linearly with the minimum number of antennas used at each side of the communication link. It should be noted that Telatar's paper was the first to connect the capacity of spatial vector communications with the singular values of the (matrix) transmission channel.

However, the MIMO concept was not entirely new though. On the information theory side, the first analysis of the MIMO channel capacity was conducted by Wyner in the 1970's. With a more engineering approach, Winters proposed several schemes for transmit diversity in mobile systems in the 1980's. Nonetheless, these schemes were not yet *space-time coding* or *spatial multiplexing*, as they are defined today. In [30] (Ch. 1), the authors, now considered pioneer researchers in MIMO, credited several past researchers for some previous work on MIMO-related concepts. A quite comprehensive history of MIMO is given in the recent introduction of [31] but still, the authors do not go beyond 2003-2004 in the historical account they give.

The explosion of publications in MIMO started[5] around 2003 (in conferences) or 2004 (in journal papers), peaking to a maximum in 2009, but even now, the number of published remains high (the data is available in the introduction of [31], and was based on IEEE publication figures). In 2003 the first widely disseminated books focused on MIMO were published by Paulraj et al. [30], by Larsson and Stoica [32] and by Vucetic and Yuan[33]. In the next few years there was a burst of book publications: in 2004 by Barbarossa [34] and by Biglieri and Taricco [35]; in 2005 by Jafarkhani [36], and one (edited) by Gershman and Sidiropoulos [37]; in 2006 (edited) by Bölcskei, et al. [38] and also by Kühn [39], in 2007 (edited) by Biglieri et al. [40], by Giannakis et al. [41], and by Duman and Ghrayeb [42]. In 2007 the book by Oestges and Clerckx [43] analyses MIMO implementation in real channels (considering antenna correlation and

[4] The results were initially presented by Telatar in 1995 in an AT&T Bell Labs technical report.

[5] The start of the publication boom is being considered here as the year when the number of publications roughly doubled in comparison with the previous year.

departing from the flat Rayleygh fading assumption). It is worth mentioning that in the 2005 textbooks on wireless communications by Goldsmith [44] and by Tse and Viswanath [45] already included thorough analysis of several aspects of MIMO systems (the latter book in much detail).

1.1.4 – MIMO in Wireless Standards

Orthogonal frequency division multiplexing (OFDM) [46] and MIMO are the two technologies (along with larger channel bandwidth) underpinning the physical layer of the fourth generation (4G) wireless networks [47], [48], [49], such as IEEE 802.16 (dubbed WiMAX [50]) and Long Term Evolution (LTE) [51], [52], [53].

In its first releases, LTE relied on MIMO mostly for the downlink (i.e., from the base station (BS) to user equipment) [54], using 4 layers in the downlink (DL). In the latest release 10 (known as LTE-Advanced[6]), the role of MIMO also became important in the uplink (UL). Indeed, MIMO is utilised in both uplink and downlink of the IEEE 802.16m standard (WiMAX profile 2.0). The LTE-Advanced release considers DL with eight layers and uplinks with up to four layers, i.e., a BS with eight or more antennas and user terminals with each 4 antennas [55], [49], [56]. Improving the detection performance with affordable complexity in terminals with 8 layers (with 8×8 antennas) is still a very important problem [57] (p.181). With these configurations LTE-Advanced achieves spectral efficiencies of 30b/s/Hz in the DL and 15 b/s/Hz in the UL [58] (p.86), [53] (p. 40), [57] (p.181).

Details on the role of MIMO in WiMAX are given in [59], [60], [61],[62], and an overview of its application in LTE is given in [63], [55], [58].

Presently, MIMO is entering the vast domestic market via 802.11n [64], [31] (ch.7), the latest generation of Wi-Fi, designed for a peak rate of 600 Mbps (using 40MHz bandwidth and 4×4 antennas), which is the first commercial product to be based in

[6] The numbering of LTE releases is a continuation of the numbering in the releases of UMTS and its enhancements (all under the 3GPPP project).

MIMO-OFDM. The same combination of MIMO-OFDM has also enabled other standards in the IEEE 802.11 universe [65], particularly those specifically designed for high throughput. Notably, the first wireless standards for data transmission rates over 1Gbps are the 802.15.3c [66] (operating at millimetre waves and using beamforming with antenna arrays) and the 802.11ac [67] (using eight parallel layers in the 5GHz band), both incorporate multiple antennas (and LDPCs). These standards, which are scheduled to be concluded by early 2013 [65], will put in to practice the dream "gigabit wireless" anticipated by Paulraj et al. in 2004 [68].

Undoubtedly, MIMO research started within wireless communication and even today it remains the most prolific research community in the field. However, it is worth noting that the concept of SM has also started to be studied for communications via (multi-modal) optical fibres [69] and, more recently, the concept of taking advantage of mutual interference has also been extended to the traditional bundles of cables in wired telecommunication networks, turning crosstalk from a nuisance into an ally and so increasing transmission capacity [60], [70], [71].

1.2 – The Different Faces of MIMO

The definition of the MIMO communication channel is clear: there is an input *vector* $\mathbf{x}$ (with N_T elements) and an output $\mathbf{y}$ is, also a *vector* (with N_R elements), which is obtained from $\mathbf{x}$ by means of a linear (matrix) transformation $\mathbf{H}$. Furthermore, the detection of $\mathbf{y}$ is perturbed by some noise *vector* of the same size.

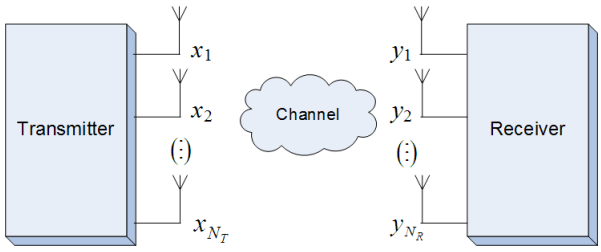


Figure 1.1: Wireless MIMO link (single-user setup).

One consequence of how fast research on MIMO developed was the emergence of a proliferation of names for the various research areas in MIMO. If sometimes the same concepts may be found disguised under different names, one may also encounter the same name associated with quite different concepts. Perhaps one important source of confusion is the existence of different terminology in academic papers and in the most important wireless standards (LTE, WiMAX and 802.11n).

It is usual to encounter specific cases where the input or the output is a one-dimensional vector; when both vectors are one-dimensional we revert to the traditional single-input single output case (SISO). Table 1.1 consists of the general taxonomy for MIMO configurations.

Table 1.1: Configurations depending in the input and output.

	SISO	MIMO	SIMO	MISO
N_T	=1	> 1	=1	> 1
N_R	=1	> 1	> 1	=1

1.2.1 – Diversity and Multiplexing

From Shannon we know that, in the AWGN channel, a symbol error rate (SER) curve $P_s(\rho)$ is a function of the signal to noise ratio (SNR), ρ, and can be as steep as one wants. In the limit, the curve $P_s(\rho)$ can have an infinite negative slope. For the Rayleigh fading[7] channel it is well known that $P_s(\rho)$ exhibits a -1 slope in the

[7] This limiting behaviour is only characteristic for the Rayleigh fading assumption. Other fading statistics lead to different diversity orders [247]. For example, under Nakagami fading, the diversity order depends on a parameter of the fading distribution which may lead to higher or lower diversity orders [246] (ch. 14), [44] (ch.6). Goldsmith points out that some measurements point out to the latter case, i.e., leading to $d < 1$ [44] (ch. 3). The existence of Rician fading (where some reflection components do not have zero mean, i.e., some dominant component exists) is usually taken as an unavoidable cause for a reduction in the diversity order. However, Lozano, Tulino and Verdú [38] (ch. 5), point out that as both N_T and N_R tend to infinity, the capacity is not changed. Note: the Rayleigh distribution is a particular case of the Rice distribution as well as of the Nakagami family.

uncoded SISO case, that is, one finds that $P_s(\rho) \propto \rho^{-1}$. One door that MIMO opens is the possibility of increasing (in modulo) that slope, i.e., obtaining a faster reduction of the error rate as SNR increases. Formally, one defines the *diversity order*, corresponding to the slope

$$d = \lim_{\mathrm{SNR}\to\infty} -\frac{\log(P_s(\rho))}{\log(\rho)}. \tag{1.1}$$

This *diversity order* measures how many statistically independent copies of the same symbol the receiver is able to receive. In brief, this amounts to the number of independent fading coefficients that the receiver can average in order to produce a reliable estimate of a transmitted symbol. Not surprisingly, the maximum available diversity that can be attained is $d_{\max} = N_T N_R$, in the case of uncorrelated fading, as in the model that will be introduced in sec. 2.2.1.

The benefits of vector communication with spatial diversity are not limited to this increased slope. Think of a SISO setup where one switches from a 4-PAM constellation (2 bit/s/Hz) to a 8-PAM constellation, in this case the same error rate can be obtained by increasing the SNR by 6dB while 1 more bit/s can be transmitted (now 3 b/s/Hz) using the same bandwidth. If one changes from a 16-QAM (4 b/s/Hz) to 64-QAM constellation, the same additional 6dB are required to achieve the same SER, though the spectral efficiency is increased by a factor of two. It is said that the *multiplexing gain* of the latter QAM constellation is higher than the one of PAM. In the MIMO general case, this gain is defined as

$$g = \lim_{\mathrm{SER}\to\infty} \frac{\log(R)}{\log(\rho)} \tag{1.2}$$

When plotting the symbol error rate (SER) versus the signal to noise ratio (SNR), the existing diversity d in the communication link is simply the slope (in the asymptotic regime) of the SER curve. On the other hand, the interpretation of the multiplexing gain in a typical SER plot is not so straightforward. The metric g indicates how the capacity increases with the SNR, which is a common representation in information theory since Shannon but is less useful in practice. In terms of the SER,

the multiplexing gain g measures how fast spectral efficiency can increase with the increase of SNR while keeping the same error rate and corresponds to the maximum number of independent *layers* or *parallel channels* and is limited by

$$g_{\max} = \min(N_T, N_R). \tag{1.3}$$

In a theoretical breakthrough paper [72], Zheng and Tse showed that there is a trade-off between d and g, i.e., the famous diversity-multiplexing trade-off (DMT): increasing one leads to a decrease in the other. The only pairs (d, g) that are allowed lie on the following piecewise-linear function constructed by connecting the points defined by

$$d(k) = (N_R - k)(N_T - k), \quad \text{for} \quad 0 \leq k \leq g_{\max}. \tag{1.4}$$

One interpretation of this trade-off is that some subset of the antennas provide for the existence of several layers, while the remaining ones assure the diversity, but they cannot all be contributing to both objectives. The operational information conveyed by the DMT curve is very often confusing and misleading in the literature. The operational meaning of the DMT curve lies in the extremities connected by each of the piecewise-linear segments. Each segment defines an operation "mode" with a pair (d, g) defined by the extremities of the segment, which then define the *maximum* value that each of the parameters can assume, as illustrated by Yao, Zhen and Wornell in [38] (ch. 8).

The practical relevance of the DMT has been much criticised though; for example, Burr in [31] (ch. 3) points out that it is only valid for the ideal (uncorrelated) Rayleigh channel and only at an impractically high SNR regime, while authors in the LTE literature rebuke the usefulness of DMT for ignoring other aspects of the transmission chain, which bring other sources of diversity for example from the frequency domain or from coding. The same argument is made by the authors of [55] and even also the authors of[53] (sec.5.6); Giannakis et al. argue that providing a physical interpretation of g in the finite SNR regions "is impossible"[41] (pp. 46-48) and recommend using an interpretation based on spectral efficiency.

Despite the connection between the two gains, there is a division in system design between either aiming at full diversity or aiming at maximising the multiplexing gain, which in practice has been measured by the spectral efficiency gain provided by the transmission over multiple layers. The development of *space-time codes* (STC) addresses the first objective, while the *spatial multiplexing* (SM) concept aims at the latter. These two concepts are presented in the following.

1.2.2 – Space-time Codes (STC)

The famous Alamouti 2×1 space-time code was presented in 1999 [73]. The scheme achieves the same diversity as MRC with two antennas at the transmitter while having only one antenna at the receiver, and transposing the burden of two antennas to the transmitter[8]. The structure of the Alamouti code permits a very simple decoding method. This advantage was extended to larger dimensions by Tarokh, Jafarkhani, and Calderbank [74], who discovered other orthogonal space-time block codes (OSTBC), which are also easy to decode owing to their structure. Interestingly, the Alamouti scheme realises the optimal trade-off for in 2×1 setup; the other OSTBC do not achieve that optimal DMT, nor does the Alamouti 2×2 configuration.

The computational complexity for their decoding was recently analysed in depth [75]. Sadly, these constructions for STBCs were shown not to exist for configurations larger than 4×4. They are however instances of linear dispersion codes which, albeit not necessarily orthogonal, also spread the symbols in both space and time. The design and study of space-time codes constitutes a research field of its own [36], [41], [32]. Another family of codes, proposed earlier than STBC, are the space-time trellis codes (STTC) [76] where the symbols emanating from the antennas not only depend on the new data but also on the state of an encoder (as in convolutional codes).

[8] There is power penalty though, given that only half of the power is collected with one antenna at the receiver rather than two. This results in a SER curve translated by 3dB in respect to MRC performance curve. The extrapolation to a 2×2 configuration of the Alamouti space-time code is straightforward and that loss is recovered.

Lattices have been essential in coding for MIMO just as they had been for the AWGN channel and afterwards for the SISO flat Rayleigh channel. A fruitful line of research, mostly lead by Oggier, Viterbo, and Belfiori, uses algebraic number theory for finding good lattice codes for MIMO [77], [78], [79]. The 2×2 so called Golden Code, which simultaneously achieves full diversity ($d = 4$) and full multiplexing gain ($g = 2$), was created under that framework. One other example of STC with lattices was the discovery by Gamal, Caire and Damen [80] of the so called lattice space-time (LAST) codes, which realise the DMT. The codes are grounded in the (previously mentioned) Erez and Zamir constructions [25]. The optimum detection algorithm for LAST codes was proposed in [81].

1.2.3 – Spatial Multiplexing (SM)

This technique focuses *only* on the objective of increasing the data rate, leaving behind rather than obtaining any spatial diversity in a $N_T \times N_R$ configuration. If the receiver is able to correctly estimate the channel matrix (even though that information is oblivious to the transmitter), signal processing at the receiver can extract the mutual interference and decouple $g_{\max}$ streams of independent data.

The first spatial technique, proposed by Foschini (as mentioned in sec. 1.1.3), was D-BLAST (diagonal Bell Labs layered space-time). This technique uses error correcting codes and "rotates" over time the distribution of the different code streams (the layers) across the antennas. Considering two dimensional space-time frames, different layers end up associated with distinct *diagonals* of a space-time grid (or frame). This creates spatial diversity besides spatial multiplexing. However, owing to the detection complexity it incurred it was dropped very early in favour of a much simpler approach known as V-BLAST (vertical BLAST). One other downside with D-BLAST is that it wastes some space-time resources at the time extremities of a frame, although one can minimise that effect by appropriately dimensioning the frames [44] (sec. 10.6). It should be noted that, despite its impracticability, when the number of antennas approaches infinity, D-BLAST is able to approach the capacity of the MIMO channel [45] (sec.

8.5). Interestingly, the V-BLAST architecture is able to approach capacity by rate adaptation across the different layers, when there is channel state information at the transmitter (CSIT) [38] (ch. 5) (for a practical example see [82]). Near capacity MIMO open loop SM has been achieved using soft sphere decoding (see Chapter 2) concatenated with linear codes by means of an interleaver [83].

V-BLAST does not make use of all the spatial diversity that exists in the MIMO channel as D-BLAST is able to. In the vertical version there exists a fixed association between the parallel sub-channels and the antennas at both extremities of the link. Note that these sub-channels are also frequently called layers, even in uncoded systems, where each layer simply corresponds to the symbols from a particular transmit antenna. Consequently, the maximum spatial diversity V-BLAST offers is, at most, N_R, and even so, only if maximum likelihood detection (MLD) is used. In the case of the ordered successive interference cancellation (OSIC) detector, the diversity is only $N_T - N_R + 1$, i.e., only one in the common case of symmetric configurations. This latter fact was conjectured about from very early on (e.g., [30] (p.158)) but has only very recently been proven [84] (this will be further commented on in Chapter 2).

Unlike the Alamouti (and other OSTBCs), both V- and D- BLAST could be trivially extended to any number of antennas, as there is no structural constraint in their design. However, to optimally detect all layers (with an error performance curve that exhibits all the diversity that these schemes still provide and with no gain penalty), involves a computational complexity that grows exponentially with the number of antennas at the receiver.

The predominance of the V-BLAST architecture made it almost synonymous with SM. Furthermore, as Golden, Foschini, et al. [85] presented a simple receiver based in interference cancelation for V-BLAST, the name became much associated to that particular detection technique. The name successive interference cancelation (SIC) will subsequently be used in this work for the concept that underlies the detection method first proposed for V-BLAST in [85]. The V-BLAST architecture will be simply referred to throughout this work as SM.

SM does not require CSIT (since it is an open loop architecture) and the capacity grows linearly with $\min(N_T, N_R)$. In practice, the number of antennas in some equipment is not only limited by the signal processing complexity at the receiver, but also by the physical dimension the antenna array may have; one should bear in mind that as the spacing between antennas diminishes, they become increasingly correlated and the capacity of the system diminishes (e.g., [30] (sec. 4.6.1).

The major limitation in SM is the large algorithmic complexity involved in the optimum detection applying the MLD principle to achieve optimum detection. MLD captures the spatial diversity of the architecture while removing all the mutual interference between layers.

In the last decade there was a burst of research on this problem: how to detect the received vector with a performance as close as possible to the optimal yet having a reduced complexity compared with MLD? The most abstract and general description of this problem is the *closest vector problem* (CVP) in a lattice, the applications of which go far beyond the MIMO detection problem in SM. The detection of some STC is also a CVP in a lattice after vectorising the space-time matrix code words [77].

Other communication problems such as inter-symbol interference (ISI) channels [86], multi-user detection (MUD)[87] are formally the same, and may be encapsulated as a general equalisation problem (as proposed in [88]), that can be mapped as a CVP.

Table 1.2 lists some terminology that is used in these different frameworks. Almost all topics in this thesis deal with several aspects of the CVP.

Table 1.2: Different names of analogous techniques.

	MIMO	**Equalisation for ISI channels**	**Multi-user Communication**
Inversion (linear)	• Zero-forcing (ZF) • Channel inversion • Decorrelation	Zero-forcing (ZF) equalisation	Decorrelating
Minimum mean squared error (MMSE)	MMSE	MMSE filtering	MMSE detection
Interference cancellation	•Nulling and cancelling • Successive interference cancellation (SIC) • V-BLAST detection	Decision feedback equalisation (DFE)	• Iterative multi-user detection (MUD) • Successive interference cancellation (SIC)
Optimum detection	• Maximum likelihood detection (MLD) • Exhaustive search	Maximum likelihood sequence detection (MLSD)	• ML detection • Brute force • Sphere decoding (near optimum)
Precoding	• Multiuser-MIMO • Broadcast channel (BC)	• ISI Precoding • Costas precoding • Tomlinson-Harashima precoding (THP)	Dirty paper coding (DPC)
Parallel sub-channels	• Closed loop SU-MIMO • Singular value decomposition (SVD) and water filling • Communication over eigen- modes [89] • Eigen-beam spatial division multiplexing • Precoding [90] • Beamforming	• OFDM • Multi-tone modulation • Filter bank multicarrier	Not defined

1.2.4– Spatial Diversity Versus Spatial Multiplexing

Physical layer designers face the problem of opting between STC and SM. Another attempt to match them under a unified system design was presented recently by El-Hajjar and Hanzo [91]. A pragmatic approach for switching between them according to the channel conditions was considered in [92].

This question was thoroughly investigated very recently by Lozano and Jindal [93]. They have looked into the problem of considering MIMO in systems that combine MIMO with interleaving and coding, wideband channelisations with OFDM, link adaptation (adaptive modulation and rate control), and automatic repeat request (ARQ). Their work addresses precisely some of the criticism aimed at the somewhat idealised conditions in which DMT was defined (as mentioned in section 1.2.1). The conclusion was that with all the diversity available in time and frequency (including carrier aggregation), spatial diversity becomes redundant and SM should be the *only* objective when designing the MIMO aspects of the physical layer, especially when the channel is wider than 10 MHz. Note that LTE release 8 defines channels bandwidths up to 20 MHz, LTE-Advanced (i.e., release 10) already defines a bandwidth up to 100 MHz [58], and 100 MHz is possible in WiMAX by carrier aggregation [59], and 802.11n is defined up to 40 MHz [64].

1.2.5 – Multi-user MIMO

The existence of multiple antennas on at least one side of the link is not limited to single-user systems (SU-MIMO); capacity gains and better complexity trade-offs also exist in multi-user MIMO (MU-MIMO) where a user terminal can have only one antenna. This becomes important when the terminal is too small to provide any room for spatial diversity or little capacity for signal processing, whist the BS can bear several antennas and handle demanding signal processing tasks.

Broadcast channel (BC): given its information-theoretical roots, this is also sometimes called *dirty paper coding*, although in the 4G literature it appears under the name of space division multiple access (SDMA) or simply *downlink MU-MIMO*. The

advantage of BC is enormous given that several *single antenna* user terminals can receive (with very little processing) its own information "cleared" from any interference from the signals intended for another terminal located elsewhere. Moreover, this is accomplished while simultaneously using the same time-frequency resources in all the users that are being served by that BS. The technique is chiefly inspired by the precoding techniques for channels with inter-symbol interference (ISI) [94] such as Tomlinson-Harashima precoding, which has been extrapolated to more than the two dimensions (the QAM case) in order to be applied to MIMO. The techniques for the BC developed in the last decade are almost entirely based on the properties of lattices [95], [96]. It is important to notice that the error performance of the BC is highly sensitive to good knowledge at the BS of the channel (CSIT) for each user terminal that it serves.

Multiple access channel (MAC): this can be seen as the dual of the broadcast scenario, where all user terminals (possibly with a single antenna) simultaneously transmit to the base station from their different locations.

The collection of the dispersed antennas in the BC and MAC are sometimes called a *virtual antenna array* (which is itself is a broader concept related with co-operative networks). Both the 802.16 family of standards [61] and LTE [54], [52] (sec. 11.2.3)) allow BC and MAC.

1.2.6 – Single-user Closed loop (Water-filling)

When there is simultaneously perfect channel state information at the transmitter (CSIT) and perfect channel state information at the receiver (CSIR), the MIMO capacity can be reached by a simple technique, simultaneously achieving full diversity and full multiplexing gain. By computing the singular valued decomposition (SVD) of the channel and adding linear filters at both the transmitter and the receiver (both filters are unitary matrices), it is possible to convert the MIMO channel into a set of parallel SISO channels and achieve capacity applying a power adaptation based on *water-filling*, according to the singular values of $\mathbf{H}$ (e.g., [35] (sec. 4.1)) (this will be

explained further in sec. 7.3). The number of channels available equals $r = \text{rank}(\mathbf{H})$, i.e., the number of non-zero singular values of the channel matrix.

In fact when CSIT exists and the channels are decoupled via SVD, the optimal DMT can be achieved. By sending different symbols through each one of the parallel channels, a multiplexing gain $g = r \leq \min\{N_T, N_R\}$, though no diversity is involved (each symbol travels in one and only one channel). The system can also be designed to operate in the other extreme of the DMT piece-wise curve, i.e., with full diversity $d = N_R N_T$. That can be achieved by "rotating" the symbols across the r channels. However, because r "channel uses" are necessary to transmit r symbols, the multiplexing gain is zero in that case.

1.2.7 – Beamforming

This technique, which is well known in many areas such as antenna theory or remote sensing, amounts to steering the transmit beam of the BS to a particular user by dynamically controlling the weighting of the transmit power in each of the elements of the antenna array. Although less common, there is one other concept that is also dubbed beamforming. However, that technique is a particular case of water-filling, corresponding to the case when only one singular value of $\mathbf{H}$ is significant. In that case all the power is assigned to that singular value and it can be shown that it also amounts to transmitting the same symbol in all antennas at the same time, though with scaling gains in each of them. Notice that this is what happens in the low SNR regime, when spreading the power through more than one singular value leads to marginal gains [42] (p.53-54).

1.2.8 – Channel Feedback

It should be pointed out that for the cases of beamforming, water-filling, and for both MU configurations, the existence of a reverse link (from the receiver to the transmitter) is essential unless the UL and DL channels are reciprocal. While channel reciprocity may occur in time division multiplexing (TDM) systems, it does not exist in

frequency multiplexing (FDM) systems. The knowledge that either the Tx or the Rx may have of the channel may be complete or partial (for example, only the distribution of the channel coefficients may be known).

A comprehensive overview of the capacities (or, the *capacity regions* in the case of MU scenarios) for most MIMO scenarios, including BC and MAC, was provided in 2003 [97]. The paper analyses all cases when both CSIT and CSIR exist, when only CSIR exists, and also the cases when the exact channel is unknown but still its probability distribution p_θ is known (which is a particular case of Figure 1.2, when knowledge of $\mathbf{H}$ is absent at Tx, at Rx or from both). Yet, the capacity of the broadcast channel (not based on the duality with the BC as in [97]) was only fully characterised later by Weingarten, Steinberg, and Shamai in 2006 [98] [9].

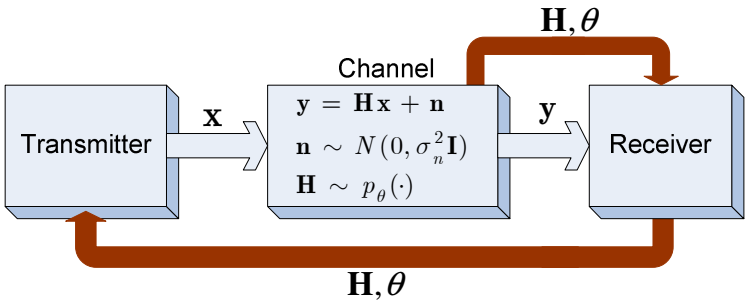


Figure 1.2: Single-user MIMO with channel state information at the receiver and at the transmitter (either full information or the distribution).

In spite of the progresses made, the case of single-user MIMO still holds some open problems regarding the capacity (under various particular assumptions), which are listed in [40] (sec.2.3.4).

Precoding for closed loop SU-MIMO with water-filing is only possible if the channel matrix is known at the transmitter. However, when for instance only the statistics is known, it is still possible to partially adapt the signal. The general techniques for all these situations were overviewed in [90].

[9] The paper received the IEEE Information Theory Paper Award in 2007.

It is clear that the performance of closed loop techniques is dependent on the accuracy of the CSIT. However, the volume of feedback information can be enormous, especially for fast changing channels, requiring many channel updates. Think of a system with a 4×4 MIMO-OFDM complex channel with 512 OFDM sub-channels, 8 bit quantisation per real value channel coefficient, 100 Hz Doppler frequency, and channel estimation at 10 times the Doppler rate. The total feedback is $16 \times 2 \times 512 \times 8 \times 100 \times 10 = 131.1$ Mb/s, which, at the present time, is a totally unreasonable data rate to allocate to a control channel.

The most common technique to reduce the transmission rate in the reverse channel is based on vector quantization and codebooks where the information transmitted identifies one element in the finite codebooks of possible channels (overviews can be found in [99] and [100]). One usual assumption is that the channel does not change during the delay involved in informing the transmitter [101]. In more recent literature, the effect of delay is also considered in the design of the feedback techniques (e.g., [89]). In the case of the BC channel it was found by Jindal[102] that the quality of feedback provided by each (single antenna) user needs to improve as the SNR of the user increases in order still to achieve the multiplexing gain (which does not happen in SU MIMO).

1.3 – Motivation and Scope

Digital transmission has progressed during the last two decades of the 20$^{\text{th}}$ century aiming at higher data rates, less bandwidth for a fixed data rate (i.e., higher spectral efficiency), while spending the least possible amount of energy per bit, given a certain additive noise. There is, however, a fourth dimension to the problem: the complexity involved in the "construction" of the transmitted signal (i.e., the complexity associated with the modulation and the coding scheme), and the complexity involved in the detection and decoding of the signal at the receiver. Typically, progress towards Shannon capacity was achieved by means of channel coding concatenated with higher-order modulation, eventually at the expense of higher complexity, mostly at the

receiver. Turbo-codes, LDPCs, and lattice-coded modulation are examples of the path of increasing complexity (mostly in detection and decoding).

The rapid rise in the computing power available at the handset now permits rather complex baseband processing. In the last dozen of years we have witnessed the core problems in communication engineering being much less electronics-centric and much more algorithmic-centric. Modern communication theory is now largely entwined with problems traditionally in the domain of theoretical computer science (e.g., machine learning, data structures, algorithms and their complexity), or, more generally, in applied mathematics (related with matrix algebra, discrete mathematics, integer programming or combinatorics). Sometimes the separation is now only barely possible by looking at the application in mind and not by the nature of the problem itself. More generally, this can also be said of many of the aspects of information theory and coding theory. The fields of image communication or source coding (compression) always incorporated a wide variety of fundamental research. What is new is that this fusion propagated to the physical layer, once clearly within electrical engineering.

The problem of detection in MIMO SM is the central one in this thesis and constitutes a clear example of an algorithmic problem at the physical layer. The problem is analogous to the (already mentioned) closest vector problem (CVP) in lattices (sometimes also called the *nearest vector problem* (e.g., [103]). The study of the problem began in the realms of computer science, cryptography, complexity theory, algorithmic number theory, and in some domains of applied mathematics. The thesis reflects that fact, and many approaches for the manipulation of lattices in MIMO presented in this work constitute an effort to extend the tools available for MIMO engineering. The reduction of the complexity of MIMO detection has been investigated throughout the last decade and entire special issues of leading journals [104] are devoted to the topic.

1.3.1– Limitations of Scope

The channel model used in this thesis is the flat, independent, and ergodic Rayleigh channel. This is the model that is pervasive in the papers published on the topic of lattice detection for MIMO SM (and indeed for STC and also for the BC). However, this model implies that channel estimation is always perfect at the receiver.

1.4 – Publications

The research presented in this dissertation led to the following publications:

- F. A. Monteiro, I. J. Wassell, "Efficient scalar quantization for MIMO spatial multiplexing receivers", in Proc. of the 9th Inter. Symp. on Communication Theory and Applications (ISCTA), Ambleside, Lake District, UK, July 2007.
- F. A. Monteiro, I. J. Wassell, "Euclidean distances in quantized spaces with pre-stored Components for MIMO detection", in Proc. of the 10th European Conf. on Wireless Technology (ECWT) – 10th European Microwave Week, Munich, Germany, Oct. 2007. (Best Paper Award – Conference Prize)
- F. A. Monteiro, I. J. Wassell, "Progressive hypercube decoding", in Proc. of the 4th IEEE Inter. Symp. on Wireless Communication Systems 2007 (ISWCS), Trondheim, Norway, Oct. 2007.
- F. A. Monteiro, I. J. Wassell, "Recovery of a lattice generator matrix from its Gram matrix for feedback and precoding in MIMO", in Proc. of the 4th Inter. Symp. on Communications, Control and Signal Processing (ISCCSP), Limassol, Cyprus, March 2010.
- F. A. Monteiro, Frank R. Kschischang, Trellis detection for random lattices, in Proc. of the 8th Inter. Symp. on Wireless Communications Systems (ISWCS), Aachen, Germany, Nov. 2011.
- F. A. Monteiro, I. J. Wassell, "Dual-lattice-aided MIMO detection for slow fading channels", in Proc. of the 11th IEEE Inter. Symp. on Signal Processing and Information Technology (ISSPIT), Bilbao, Spain, December 2011.

  Other:

- F. Monteiro, "Faster and faster: a look at the remarkable achievements in error-free digital communications", BlueSci, Cambridge, April 2009.

1.5 – Dissertation Outline

The structure of this thesis is as follows:

Chapter 2 introduces the detection problem in spatial multiplexing as a *closest vector problem* (CVP) in a Gaussian lattice whose optimal solution (MLD) is NP-hard. It presents the simplest (largely sub-optimal) linear receivers and the two best solutions known: lattice reduction-based receivers and sphere decoding.

Chapter 3 looks at the traditional linear receivers and at successive interference cancelation (SIC) receivers from a geometric perspective. In particular, an interpretation of the optimal ordering in SIC detection is given. The chapter makes a connection between the geometry of the primal and dual lattices and proposes a receiver exploring the information provided by the dual lattice.

Chapter 4 presents a technique for reducing the implementation complexity of receivers that tackle lattice detection with MLD-inspired techniques when the dimensionality of the computational problem is still bearable for methods based on exhaustive search.

Chapter 5 introduces some tools for the description and analysis of lattices under algorithmic number theory and group theory frameworks that allow different ways of defining a lattice.

Chapter 6 argues that the CVP in random lattices can be near-optimally solved by linearly mapping the lattice onto a synthetic lattice that is constructed to be simultaneously "nearby" to the given lattice and also be a member of the family of lattices holding a trellis representation. It is shown how that representation of the synthetic lattices is associated with their group-based coset decomposition.

Chapter 7 proposes the use of the LDL^T decomposition for the purpose of delivering CSI to the receiver for closed loop architectures.

Chapter 8 is an overview of the contributions in the dissertation and looks into other problems that may benefit from the analysis presented in this work.

Chapter 2 – Fundamentals on Lattices and Spatial Multiplexing

"Lattices are everywhere."
Ram Zamir [105]

"It is not known that these things can't be solved in polynomial time. It is thought that's the case. And it may be that at some point, somebody will show that you can't solve, these really are harder... However, I think there is an insurance policy (...). A ton of super smart people have worked on all these problems, and now all these things are banded together, as you would do with an insurance, so if tomorrow somebody, probably a Russian, proves P=NP (...) would indeed be embarrassing for a lot of people, however the embarrassment is amortised across a huge (...) a great swaff of people, basically people in computer science and stuff like that. So it is thought that they're really hard. But if they're not, then you're in very good company with people who also thought they were hard."
Stephen Boyd, Convex Optimization Lectures,
[Stanford University, online (1st lecture, 30')]

2.1 – Lattices

This chapter begins with a description of lattices. After listing some of the problems they can be related to, they are defined along other useful concepts to this work. Later,

the detection problem in spatial multiplexing will be shown to be closely linked to a lattice problem.

2.1.1 – Context

The regularity of a lattice lends itself for the representation of problems where signals are interpreted as a point in a multidimensional space defined in some basis. One of the most important lattice problems is the closest vector problem (CVP) [106], which consists in finding the point that is the one at the shortest distance from a given off-lattice target point.

The study of lattices began in the 1890s with Minkowski who created the then new field of *geometry of numbers* [107], [108]. Lattices are related with problems in the integer domain, such as: continued fractions, simultaneous Diophantine equations (systems of questions where one is solely interested in integer solutions) [109]; simultaneous Diophantine approximation [110], [103], (finding the closest rational numbers to a set of real numbers with the restriction that they all have the same denominator), and several other fundamental problems in number theory [103], [111], and in integer programming [109], [112]. These problems can usually be reduced to the CVP or to the shortest vector problem (SVP) in a lattice [113].

In the last three decades one could have found applications of lattices in vector quantization and image coding [114], [115], [116] and, as mentioned in Chapter 1, the application of lattices in SISO communications has a long history in coding for the bandwidth-limited AWGN channel [117] and in SISO fading channels [24]. Despite that, it was only during the boom of research in MIMO in the last decade that lattices started to be thoroughly investigated in relation to communication problems as they are the mathematical object underlying problems such as the broadcast channel [118], the design of STCs [77], and, of course, the CVP in SM detection [119]. Interestingly, these MIMO communication problems triggered a series of re-discoveries and novel uses of ideas previously studied in algorithmic number theory. Examples of this are i) the V-BLAST detection as proposed in [120], which turns out to be the Babai nearest plane

algorithm [121], [122]; ii) sphere decoding was already used in SISO [123] but improved ways for traversing a tree were rediscovered in [106] making use of the much earlier findings of Fincke and Pohst [124] and by Schnorr and Euchner [125] in number theory; iii) the use of lattice reduction techniques such as the Lenstra-Lenstra-Lovász (LLL or L^3) algorithm or Seysen's reduction remained unknown to the communications community until 2002 [126] and 2007 respectively (the advantages of Seysen's reduction for MIMO were simultaneously indicated by [127] and [128]). However, in 2007 the 25th anniversary of the LLL algorithm was celebrated by the algorithmic number theory community with a special event and the publication of a book listing its profound implications in many problems [129].

Now that communication theory is evolving from point-to-point transmission problems to network coding ideas, lattices remain an essential tool [130], [131].

Even though lattices are simple to define mathematically, and have an apparent geometrical simplicity, they are, as already mentioned, closely related to many of the most difficult algorithmic problems with NP-hard complexity. As a natural consequence, lattice problems also assumed a central role in cryptography in the last decade [132], [113], given the complexity of the algorithms and the difficulty they pose to an attacker who does not possess a trapdoor to solve the problem (such as a "good" basis for the lattice).

2.1.2 – Basic Definitions

Lattice

There are several ways of specifying a lattice[10] Λ . The most common method involves a set of linearly independent *generator vectors* $\mathbf{h}_i$ [107], which constitute a *basis* for the lattice. A (real) lattice is then defined as the infinite set defined by

[10] The term lattice has two meanings in mathematics. The same name appears in order theory (in discrete mathematics and abstract algebra) [209], [248], a subject totally unrelated to the lattices in number theory and the geometry of numbers.

$$\Lambda = \left\{ \mathbf{y} \in \mathbb{R}^n : \mathbf{y} = \sum_{i=1}^{n} \mathbf{h}_i x_i = \mathbf{H} \cdot \mathbf{x} \,, \quad x_i \in \mathbb{Z} \,, \mathbf{h}_i \in \mathbb{R}^n \right\}. \tag{2.1}$$

The definition can be extended to complex lattices but, because it is possible to transform any complex lattice into a real lattice (as will be seen in section 2.2.2), one can settle for limiting the description to real lattices.

The integer combination of real or complex n-dimensional vectors generates a discrete set of points with the properties of a *group*, namely: *closure*, *associativity*, *identity* and *inversion* [133] (ch.20). Indeed, the shortest possible definition of a (real) lattice is the following: a lattice is a *discrete* Abelian (i.e., additive or commutative) subgroup of $\mathbb{R}^n$. The two definitions are equivalent [134] (p. 44).

A consequence of the last definition given for Λ is that for any two elements $\mathbf{x}, \mathbf{y} \in \Lambda$, then the difference $\mathbf{x} - \mathbf{y} \in \Lambda$ (i.e., a lattice is closed under subtraction). Notice that for a structure to be a lattice, the group property by itself does not suffice; the structure also needs to be *discrete* (i.e., for each lattice point there exists a hyper-ball with radius $\varepsilon > 0$ which is centred at the lattice point, not containing any other lattice point inside; that is, the distance between lattice points is larger than ε). This caveat is sometimes forgotten by some authors. For example, the group property is preserved the linear projection operator. However, that projection is not necessarily constituted by discrete structure [135] (p20).

According to (2.1), a lattice is an infinite set of points resulting from integer combinations of the columns of the generator matrix $\mathbf{H}$. It should be noted that some authors prefer to span the row space of a matrix, which then reflects algebraically in some of the definitions that follow.

There are other ways of specifying a lattice that do not have a set of generator vectors (as it will be shown in Chapter 5); however, (2.1) is the most prevalent one while these other techniques remain largely unmentioned in the literature on lattices. In MIMO literature, (2.1) is the only way used for specifying a lattice, perhaps because it follows directly from the natural vector description of SM. In [103] (sec. 4), Hendrik Lenstra describes several alternative ways of specifying a lattice but comments that

some are recognisably difficult to convert into (2.1) or even to convert between themselves. None of the unconventional techniques seem to have played any role so far in the study of MIMO.

One of the alternative techniques to define a lattice is only applicable to the so-called *cyclic lattices*. These lattices are endowed with a specific structure that allows them to be defined by means of one modular equation (lattices with one cycle) [136] or by d modular equations (said to have d -cycles) [137]. Interestingly, there is a connection to the field of numerical integration of multidimensional functions where cyclic lattices are closely related with the so-called *lattice rules* [138]. Chapter 5 will analyse how cyclic lattices relate to the lattices in the independent and identically distributed (i.i.d.) Rayleigh channel.

Fundamental Region

Given a certain basis of a lattice, the *fundamental region* that is associated to that basis is defined as

$$\mathcal{R}(\mathbf{H}) = \left\{ \mathbf{Hx} : 0 < x_i < 1 \right\}. \tag{2.2}$$

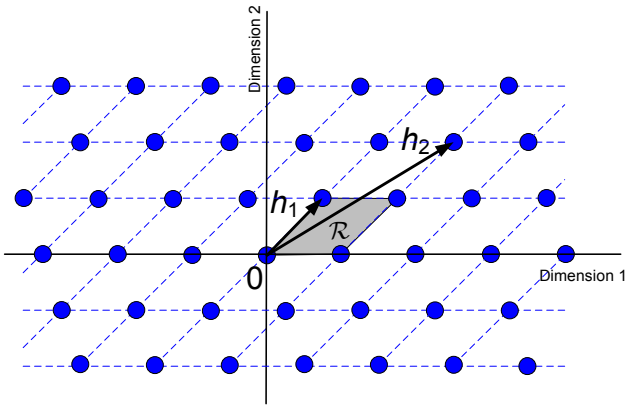


Figure 2.1: A lattice in $\mathbb{R}^2$ and the fundamental region associated with a particular basis.

The fundamental region cannot contain any lattice point inside it. If there was at least one point inside, it could not be represented by an *integer* combination of generator vectors, which are precisely the sides defining that fundamental region (c.f. Figure 2.1). If that happens, then the set of vectors is *not* a basis of the lattice but a

basis of one of its *sublattices*. A sublattice Λ' is also a lattice and the volume is $\mathrm{vol}(\Lambda') > \mathrm{vol}(\Lambda)$ (the technical definition of the volume of a lattice will shortly be given).

Note that different sets of vectors may generate the same lattice. Indeed, the number of admissible bases for a lattice is infinite; it is easy to infer from Figure 2.1 that it is always possible to select some point further distant from the origin to replace a generator and still have a fundamental region without including any lattice point in its interior. Moreover, all these different bases are related by unimodular transformations, as it will be described below.

Voronoi Region

The region of the space where the lattice is embedded that contains all the points in the span of the lattice (i.e., in the continuous Euclidian space where the lattice exists) which are closer to a given lattice point $\mathbf{x}$ than to any other point in the lattice is called the *Voronoi region* and is defined by

$$\mathcal{V}(\Lambda) = \left\{ \mathbf{z} \in \mathrm{span}(\Lambda) : \forall \mathbf{y} \in \Lambda \left\| \mathbf{x} - \mathbf{z} \right\| < \left\| \mathbf{y} - \mathbf{z} \right\| \right\}. \tag{2.3}$$

This (open) region is a characteristic of the lattice and independent of any particular generating matrix, and is the most interesting fundamental region amid the infinite number of other possible fundamental regions one can define to tile the entire space as it constitutes the optimal decision region for the closest vector problem in a lattice.

Gram Matrix

The *Gram matrix* of a lattice defined by the columns of $\mathbf{H}$, as in (2.1), is defined by (in the real case transposition replaces the Hermitian operator)

$$\mathbf{G} = \mathbf{H}^H \mathbf{H}. \tag{2.4}$$

By construction, the Gram Matrix contains all the possible inner products between all the generator vectors: $g_{ij} = \left\langle \mathbf{h}_i, \mathbf{h}_j \right\rangle$; in particular, the diagonal elements are the squared norms $\left\| \mathbf{h}_i \right\|^2$. This fact implies that $\mathbf{G}$ is Hermitian and positive definite. Moreover, it defines a positive definite quadratic form (e.g. [139], sec. 7.6) because

$$\begin{aligned}\left\|\mathbf{y}\right\|^2 &= \left\|\mathbf{Hx}\right\|^2 = (\mathbf{Hx})^H(\mathbf{Hx}) = \mathbf{x}^H\mathbf{H}^H\mathbf{Hx} \\ &= \mathbf{x}^H\mathbf{Gx} = \sum_{i=1}^{n}\sum_{j=1}^{m} g_{ij}x_i\overline{x}_j \geq 0, \text{ for all } \mathbf{x} \neq \mathbf{0},\end{aligned} \tag{2.5}$$

where $\overline{x}_i$ denotes the conjugate of x_i and $\mathbf{0}$ is the zero vector. Like the Voronoi region, the Gram matrix is another invariant of a lattice in respect to a particular basis.

Volume

When $\mathbf{H}$ is non-singular, the lattice is full-rank. In that case the *volume* of the lattice (the volume of $\mathcal{R}$) is

$$\text{vol}(\Lambda) = \left|\det(\mathbf{H})\right|, \tag{2.6}$$

however, for rectangular $\mathbf{H}$, the following more general definition is required:

$$\text{vol}(\Lambda) = \sqrt{\det(\mathbf{H}^H\mathbf{H})} = \sqrt{\det(\mathbf{G})}\,. \tag{2.7}$$

The volume of the lattice is also an invariant of the lattice, i.e., is independent of the choice of basis.

Unitary, Orthogonal, and Unimodular Matrices

An $n\times n$ *unitary* matrix $\mathbf{U}$ has complex entries and $\mathbf{U}^H\mathbf{U} = \mathbf{I}$ (i.e., the identity matrix) and its determinant is $\det(\mathbf{U}) = \pm 1$ (positive values account for rotations and negative values account for the existence of reflections). An *orthogonal* matrix $\mathbf{Q}$ has real entries and $\mathbf{Q}^T\mathbf{Q} = \mathbf{I}$. Both unitary and orthogonal matrices form a group[140]. A *unimodular* matrix $\mathbf{M}$ is a square matrix with *integer entries* and with determinant $\det(\mathbf{M}) = \pm 1$ [141], [109] (sec. 4.3). The inverse of a unimodular matrix is also unimodular (this is because these matrices also form a group [134] (sec. XV, p. 148). Unimodular matrices can always be generated by starting from an identity matrix and successively applying any of the following *elementary column operations* (or row operations according to the convention):

i) Change signs of all the elements in a column;
ii) Swap two columns;
iii) Add and integer multiple a of one column to another columns.

Examples for these three cases are, respectively:

$$\text{i) } \mathbf{M}=\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}; \qquad \text{ii) } \mathbf{M}=\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}; \qquad \text{iii) } \mathbf{M}=\begin{pmatrix}1 & 2 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \text{ where } a=2\,.$$

All these three elementary operations which can generate any unimodular matrix have clear geometric interpretations, but for that purpose the notion of lattice equivalence up to scaling, orthogonal and unimodular transformations will be first introduced.

Equivalent lattices

It has already been mentioned that a basis is not unique. Furthermore one can observe that a scaled or rotated version of a lattice is isomorphic to it, and therefore, in a geometric sense, is equivalent to it. One defines then the notion of lattice equivalence. A complex lattice generated by a basis $\mathbf{H}$ is equivalent to a lattice defined by a matrix $\widehat{\mathbf{H}}$ if and only if

$$\widehat{\mathbf{H}}=c\cdot\mathbf{U}\cdot\mathbf{H}\cdot\mathbf{M}\,, \tag{2.8}$$

where $\mathbf{U}$ is a unitary matrix and $\mathbf{M}$ is a unimodular matrix and $c\in\mathbb{R}$. By applying a real model (to be defined in section 2.2.2), one can henceforth deal instead with $n\times n$ orthogonal matrices $\mathbf{Q}$ instead of unitary $\mathbf{U}$.

As Agrell pointed out in [116], if $\mathbf{U}$ is known and $\mathbf{M}$ is not known, it is easy to show that the lattices are the same. One option is to compute the (unique) Hermite Normal Form (HNF) for both bases and verify if both HNF are the same (Chapter 5 will detail these aspects). One alternative to this method would be to write each vector in one of the bases as an integer combination of the vectors in the other basis - as hinted by Micciancio in [113] (p.19). Knowing $\mathbf{M}$, it is also possible to find which orthogonal (unitary, in the complex model) matrix $\mathbf{Q}$ would transform one basis into the other by framing the problem as the Procrustes orthogonal problem [142], [143], [144]. Note that the QR decomposition is unique up to the sign of the elements in the diagonal (e.g., [106]). Hence, one alternative to the problem of finding $\mathbf{Q}$ would be to compute the QR decomposition of both matrices ($\mathbf{H}$ and $\widehat{\mathbf{H}}$) and verify that the $\mathbf{R}$ triangular matrix in both cases was the same up to the negation of its columns.

The Geometry of Unimodular Transformations

While the first two kind of elementary unimodular operations, i) and ii), change the sign of the determinant of the lattice, they do not change its modulo. In other words, they can include reflections but the volume remains the same. The concept of operation iii) is illustrated in Figure 2.2 for a 2D case and with $a = 2$.

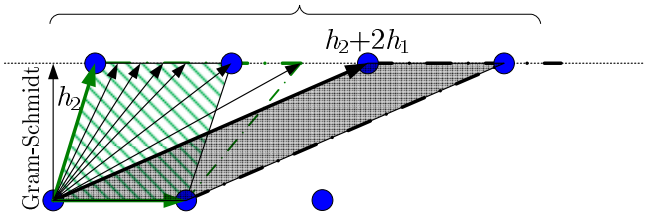


Figure 2.2: The elementary operation that skews the fundamental region of a lattice preserves the determinant. The two shaded areas are the same.

It is easy to see that the determinant of the lattice remains unchanged after the later type of elementary operation too. It should be noted that if the restriction on $a \in \mathbb{Z}$ is dropped and a is allowed to be real, the volume of the associated region also remains unchanged. In fact, the volume is solely dependent on the length of the Gram-Schmidt orthogonalised vectors. However, it should be noted that when $a \notin \mathbb{Z}$, the new set of vectors *no longer* constitutes a basis for the lattice as the vector may no longer lie on the lattice.

Shortest Vector and Successive Minima

Lattices have a shortest vector (and at least its symmetrical with the same norm). Many times one is interested in finding the shortest vectors that are also linearly independent (so that a vector and its symmetrical cannot be both considered). Hence, λ_i is the i^{th} *successive minimum* of a lattice if λ_i is defined as the smallest real number which is the smallest radius of a sphere containing i pairwise independent vectors, all with norms smaller or equal to λ_i. The shortest vector clearly has norm λ_1.

2.1.3 – The Dual Lattice

Every lattice has a *dual lattice*[11] (the first being known as the *primal lattice*). The dual lattice is traditionally defined for real lattices, though the definition has also been extended to complex lattices [145]. Given the intuitive geometrical interpretation that is possible, in the real domain, given a primal lattice Λ with a basis $\mathbf{H}$, the dual lattice is defined as

$$\Lambda_D = \left\{ \mathbf{z} \in \mathbb{R}^n : \left\langle \mathbf{z}, \mathbf{x} \right\rangle \in \mathbb{Z} \quad , \forall \mathbf{x} \in \Lambda \right\}. \tag{2.9}$$

The dual lattice can be expressed in terms of the dual basis $\mathbf{H}^{(D)}$ as

$$\Lambda_D = \left\{ \mathbf{z} \in \mathbb{R}^n : \mathbf{z} = \underbrace{\left(\mathbf{H}^+\right)^T}_{\mathbf{H}^{(D)}} \mathbf{x}\,, \quad \mathbf{x} \in \mathbb{Z}^n \right\}. \tag{2.10}$$

where $\mathbf{H}^{(D)}$ involves the Moore-Penrose pseudo-inverse (to be defined in Chapter 3).

$$\begin{aligned} \mathbf{H}^{(D)} = (\mathbf{H}^+)^T &= \left(\left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{H}^T \right)^T \\ &= \mathbf{H}\left((\mathbf{H}^T\mathbf{H})^{-1} \right)^T = \mathbf{H}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}. \end{aligned} \tag{2.11}$$

Note that there is a unique dual lattice for each primal lattice. However, because a lattice holds an infinite number of bases, there is also an infinite number of bases for its dual, always observing $\mathbf{H}^{(D)} = (\mathbf{H}^+)^T$, in the case of real lattices, as given in (2.10).

Consider the case of full rank real matrices. In fact, for $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}^n$,

$$\left\langle \mathbf{z}, \mathbf{y} \right\rangle = \mathbf{z}^T\mathbf{x} = \underbrace{\left(\mathbf{H}^+\right)^T \mathbf{x}_1}_{\mathbf{z} \in \Lambda^{(D)}} \underbrace{\mathbf{H}\mathbf{x}_2}_{\mathbf{y} \in \Lambda} = \mathbf{x}_1^T\mathbf{H}^+\mathbf{H}\mathbf{x}_2 = \mathbf{x}_1^T\mathbf{x}_2 \in \mathbb{Z}.$$

It is also possible to show that each point in the dual lattice can be written as an integer combination of the columns of $\mathbf{H}^{(D)}$. Denoting the rows of $\mathbf{H}^{-1}$ by $\mathbf{r}_1, \mathbf{r}_2, \cdots, \mathbf{r}_n$, for any point $\mathbf{z} \in \Lambda^{(D)}$ it is possible to write

[11] The dual lattice appears in the literature also as the *polar lattice* or, more commonly, as the *reciprocal lattice*. All these names were already in use in 1971 [108] (p.24). Since then, the name polar fell into disuse, though reciprocal is a name that is still common to be found in the literature.

$$\begin{aligned}\mathbf{z}^T &= \mathbf{z}^T\mathbf{H}\mathbf{H}^{-1} \\ &= (\underbrace{\mathbf{z}^T\,\mathbf{h}_1}_{\in\mathbb{Z}})\mathbf{r}_1 + (\underbrace{\mathbf{z}^T\,\mathbf{h}_2}_{\in\mathbb{Z}})\mathbf{r}_2 + \cdots(\underbrace{\mathbf{z}^T\,\mathbf{h}_n}_{\in\mathbb{Z}})\mathbf{r}_n,\end{aligned} \tag{2.12}$$

which shows that the point in the dual lattice is defined by a linear combination of the rows of $\mathbf{H}^{-1}$, i.e., a linear combination of the columns of $(\mathbf{H}^{-1})^T$. These arguments can be extended to the cases where the Moore-Penrose inverse is required and also to complex lattices.

One interesting relation between the two bases is that

$$\left(\mathbf{H}^{(D)}\right)^T \mathbf{H} = \mathbf{I}\,, \tag{2.13}$$

which is equivalent to saying that $\left\langle \mathbf{h}_i, \mathbf{h}_j^{(D)} \right\rangle = \delta_{i,j}$, using the Kronecker delta.

The volumes of the primal and the dual lattice are related by

$$\mathrm{vol}\left(\Lambda_D\right) = \frac{1}{\mathrm{vol}\left(\Lambda\right)}\,, \tag{2.14}$$

and their Gram matrices are related by

$$\begin{aligned}\mathbf{G}^{(D)} = \left(\mathbf{H}^{(D)}\right)^T \mathbf{H}^{(D)} &= \left(\left(\mathbf{H}^{-1}\right)^T\right)^T \left(\mathbf{H}^{-1}\right)^T \\ = \mathbf{H}^{-1}\left(\mathbf{H}^T\right)^{-1} &= \left(\mathbf{H}^T\mathbf{H}\right)^{-1} = \mathbf{G}^{-1}.\end{aligned} \tag{2.15}$$

Obviously, the dual of the dual lattice is the primal lattice itself. The geometry of the dual lattice is closely related to the geometry of the primal lattice. The connection is that each point in the dual lattice defines a family of parallel (n–1) dimensional hyperplanes, where translates of an (n–1)-dimensional sublattice lie. The union of those planes captures all the points of the primal lattice. This means that the shortest vector in the dual lattice will define the most distant (n–1)-dimensional hyperplanes, whose union builds up the whole primal lattice. These hyperplanes can be interpreted as parallel layers and (as a consequence of being the ones farthest apart) are the densest ones in the lattice. In MIMO literature, the geometrical interpretation of the dual lattice as a tool for improving detection seems to have been first noted in [106] (p.

2207) for sphere decoding, and then in [145] for SIC,[146], though it is also implied in the detector in [147] (p. 1944).

From the definition in (2.9), for both Λ and $\Lambda^{(D)}$ in n dimensions, the inner product between some given point $\mathbf{z}$ in the dual lattice and any vector in the primal lattice is always an integer. Therefore,

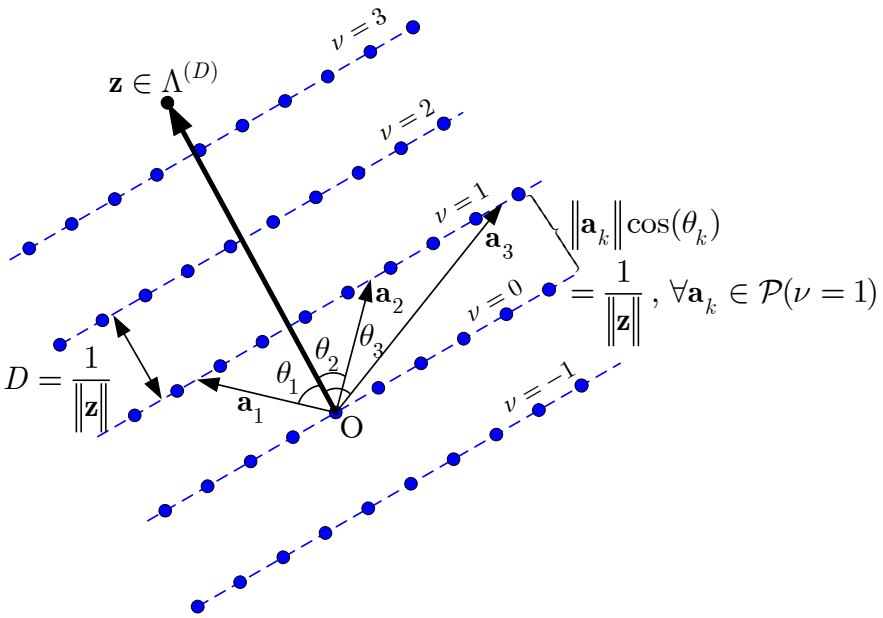


Figure 2.3: A primal lattice in n dimensions as the union of translates of a sublattice and these translates lie on $(n-1)$-dimensional hyperplanes.

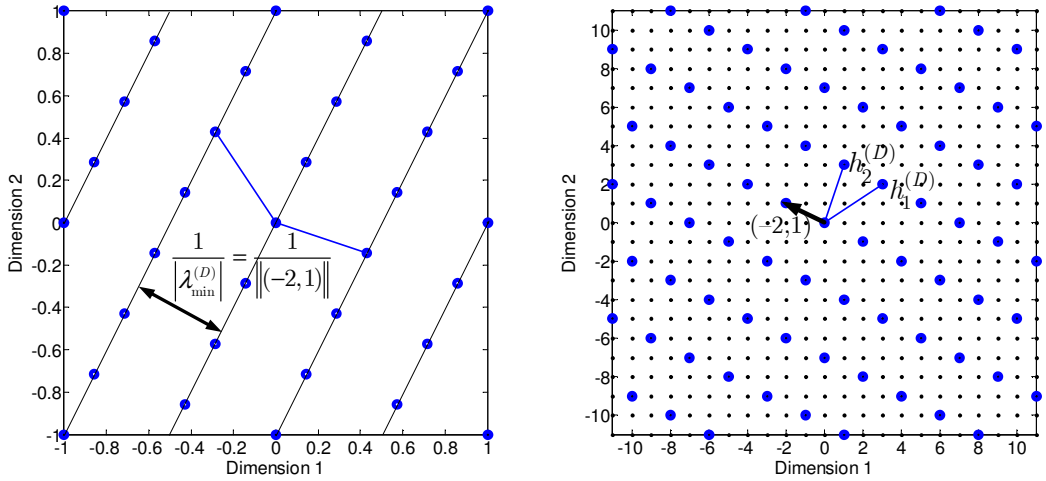
$$\begin{aligned} &\left\langle \mathbf{z}, \mathbf{x} \right\rangle \in \mathbb{Z}, \quad \mathbf{z} \in \Lambda^{(D)}, \mathbf{x} \in \Lambda \\ \Leftrightarrow &\left\| \mathbf{z} \right\| \left\| \mathbf{x} \right\| \cos(\theta) = \left\| \mathbf{z} \right\| \mathrm{Proj}_{\mathbf{e}_z}(\mathbf{x}) \in \mathbb{Z}, \end{aligned} \tag{2.16}$$

where $\mathbf{e}_z = \mathbf{z} / \left\| \mathbf{z} \right\|$.

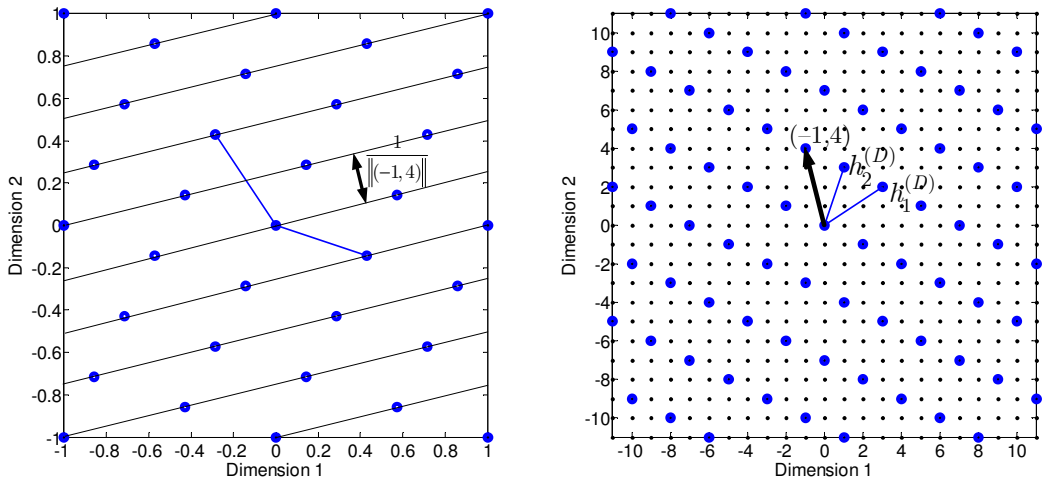
From (2.16), it is then possible to define a family of parallel hyperplanes $\mathcal{P}(\nu)$, for $\nu \in \mathbb{Z}$, such that $\mathrm{Proj}_{\mathbf{e}_z}(\mathbf{x}) = \left\| \mathbf{z} \right\|^{-1} \nu$. These are planes in dimension $n-1$ with a distance $D = \left\| \mathbf{z} \right\|^{-1}$ between them, as illustrated Figure 2.3. Note that vectors $\mathbf{a}_1, \mathbf{a}_2$, $\mathbf{a}_3$ all have the same projection onto the vector $\mathbf{z}$ that defines the set of parallel hyperplanes that is shown. ν is then the index of the hyperplane in respect to the distance between hyperplanes, i.e., $D = \left\| \mathbf{z} \right\|^{-1}$.

Figure 2.4 shows an example of two different partitions (i.e. a family of parallel hyperplanes) of a lattice associated with two different choices of vectors of the dual lattice. The example is set for

$$\mathbf{H} = \begin{bmatrix} 3/7 & -2/7 \\ -1/7 & 3/7 \end{bmatrix} \quad \text{and} \quad \mathbf{H}^{(D)} = \begin{bmatrix} 3 & 1 \\ 2 & 3 \end{bmatrix}.$$



(a) Selection of (−2,1) in the dual lattice.



(b) Selection of (−1,4) in the dual lattice.

Figure 2.4: Identification of the hyperplanes in the primal lattice (on the left side) associated with a certain point in the dual lattice (on the right side).

2.2– MIMO Spatial Multiplexing

2.2.1 – System Model

In MIMO SM with N_T transmit antennas and N_R receive antennas (with $N_R \geq N_T$), the relation between the transmitted (input) vector $\mathbf{x}_c = \left[x_{c,1}, x_{c,2}, \ldots, x_{c,N_T}\right]^T \in \mathbb{C}^{N_T \times 1}$ and the received (output) vector $\mathbf{y}_c = \left[y_{c,1}, y_{c,2}, \ldots, y_{c,N_R}\right]^T \in \mathbb{C}^{N_R \times 1}$ is modelled in the baseband as

$$\mathbf{y}_c = \mathbf{H}_c \mathbf{x}_c + \mathbf{n}_c, \tag{2.17}$$

where $\mathbf{H}_c \in \mathbb{C}^{N_R \times N_T}$ is the channel matrix, with its entries h_{ij} representing the complex coefficient associated with the SISO link between he i^{th} Rx antenna and the j^{th} Tx antenna, and with $h_{i,j} \sim \mathcal{N}_c(0,1)$, i.e., taken from a zero-mean circularly symmetric complex Gaussian distribution with unitary variance (i.e., variance 1/2 in both the real and imaginary components). The phase of these elements is uniformly distributed in [0 2π], and their amplitude has a Rayleigh distribution. This corresponds to the i.i.d. (independent and identically distributed) Rayleigh fading channel model. The subscripts denote that the elements in the vectors and the entries in $\mathbf{H}_c$ are all complex variables. Furthermore, there is noise added to each entry of the received vector, modelled by the column vector $\mathbf{n}_c = \left[n_{c,1}, n_{c,2}, \ldots, n_{c,N_R}\right]^T \in \mathbb{C}^{N_R \times 1}$ with independent circularly symmetric complex Gaussian random variables taken from $\mathcal{N}_c(0, \sigma_n^2)$, i.e., with zero average and variance σ_n^2 (corresponding to a variance $\sigma_n^2 / 2$ in both real and imaginary components). This noise model is often dubbed in MIMO literature as zero-mean spatially white (ZMSW) noise (e.g., [44]). For independent input data, its covariance is $\mathbf{R}_x = E\{\mathbf{x}_c \mathbf{x}_c^H\} = \sigma_x^2 \mathbf{I}_n$. Similarly, the covariance of the independent noise vector is $\mathbf{R}_n = E\{\mathbf{n}_c \mathbf{n}_c^H\} = \sigma_n^2 \mathbf{I}_n$. Henceforth the subscript in $\mathbf{I}_n$ will be abandoned.

It should now be clear that with integer input symbols $\mathbf{x}$, any of these possible vectors is a point on the $\mathbb{Z}^n$ lattice. The effect of the channel is that of warping $\mathbb{Z}^n$ according to the linear transformation $\mathbf{H}_c$.

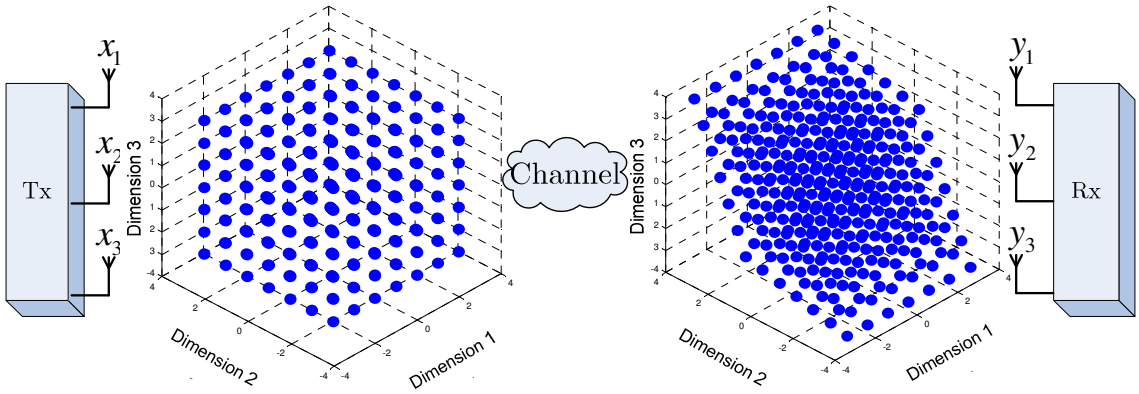


Figure 2.5: Spatial multiplexing with real inputs. $\mathbb{Z}^n$ is transmitted and then skewed by the effect of the channel.

Both PSK (phase shift keying) or QAM (quadrature amplitude modulation) constellations cam be used in MIMO, however, only the later lends itself for a lattice interpretation and most of the literature on MIMO SM concentrates on QAM, which is also the modulation that is considered in this dissertation. Consequently, the input symbols in each transmit antenna are taken from a finite complex constellation $\mathcal{A}_c$, which is some M-ary QAM (quadrature amplitude modulation). The symbols have zero mean, so that $E\{\mathbf{x}_c\} = 0$. This complex constellation is constructed from the Cartesian product $\mathcal{A}_c = \mathcal{A} \times \mathcal{A}$, where $\mathcal{A}$ is the real alphabet

$$\mathcal{A} = \left\{-(\sqrt{M}-1)a, \cdots, -5a, -3a, -a, +a, +3a, +5a, \cdots + (\sqrt{M}-1)a\right\}. \tag{2.18}$$

Traditionally, $a = 1$, and the alphabet in each real dimension is

$$\mathcal{A} = \left\{-(\sqrt{M}-1), \cdots, -5, -3, -1, +1, +3, +5, \cdots + (\sqrt{M}-1)\right\}. \tag{2.19}$$

Without loss of generality, one can assume Rx filters with impulse response $h(t)$ normalised to $\int \left|h(t)\right|^2 dt = 1$, and therefore, the *average energy* of the complex symbols in $\mathcal{A}$ is given by

$$E_s = E\left[|\, x_{c,i}\,|^2\right] = \frac{1}{M}\sum_{x_{c,i}\in\mathcal{A}} |\, x_{c,i}\,|^2 = \frac{1}{M}\sum_{x_{c,i}\in\mathcal{A}} (\Re x_{c,i})^2 + (\Im x_{c,i})^2\,, \tag{2.20}$$

which coincides with their *average power* ($E_s = \sigma_x^2$). Table 2.1 lists the values of E_s for the modulations used later in this work.

Table 2.1: Symbol energy for the used modulations.

	QPSK	16-QAM	64-QAM
E_s	2	10	42

The "overall" SNR at the receiver (Rx) is

$$\rho \triangleq \frac{E\left\{\left\|\mathbf{y}\right\|^2\right\}}{E\left\{\left\|\mathbf{n}\right\|^2\right\}} = \frac{E\left\{\left\|\mathbf{H}_c\mathbf{x}\right\|^2\right\}}{E\left\{\left\|\mathbf{n}\right\|^2\right\}} = \frac{E\left[\sum_{i=1}^{N_R}\sum_{j=1}^{N_T}\left|h_{c,i,j}x_j\right|^2\right]}{E\left[\sum_{i=1}^{N_R} n_c^2\right]} = \frac{N_T N_R \sigma_x^2}{N_R\sigma_n^2} = N_T\,\frac{\sigma_x^2}{\sigma_n^2}\,. \tag{2.21}$$

which is actually the same as N_T times the SNR of a SISO (single-input single-output channel). This comes from the fact that each antenna receives the incoming power from N_T antennas, while each receive antenna perceives the same amount of noise as in SISO. The result is valid on *average* and only when $h_{i,j} \sim \mathcal{N}_c(0,1)$, i.e., each y_i receives the sum of N_T symbols weighted by unit power random variables ($E[|\, h_{ij}\,|^2] = 1$) . Particular channel realisations will lead to different instantaneous SNRs. In this dissertation, when assessing the performance of a receiver, the SER will be plotted against the SNR as defined in (2.21). One other important metric that will appear in the capacity formula is the *SNR per transmit antenna*, which is

$$\rho_a = \frac{\rho}{N_T} = \frac{\sigma_x^2}{\sigma_n^2}\,. \tag{2.22}$$

This latter normalised SNR is in fact the same as E_s/N_0 (where N_0 is the unilateral power spectral density of the noise) because, assuming the Nyquist bandwidth and a *raised-cosine filter*,

$$\frac{\sigma_x^2}{\sigma_n^2} = \frac{E_s / T}{N_0 \cdot B} = \frac{E_s R}{N_0 B} = \frac{E_s}{N_0}. \tag{2.23}$$

Unlike what happens in SISO systems, in MIMO most performance results are given as a function of the SNR. However, some literature uses the average energy per bit[12], $E_b = E_s / \log_2(M)$, and the unilateral spectral density of noise, N_0. Accordingly the SNR given by (2.21) is the same as

$$\rho = N_T \frac{E_s}{N_0} = N_T \log_2(M) \frac{E_b}{N_0}, \tag{2.24}$$

which allows comparisons across the two different approaches seen in the literature.

It is also worth mentioning that an equivalent model for SM assuming unit noise variance and unit E_s is also often found in the literature. Maintaining all that was said for the SNR, this model must be written as

$$\mathbf{y}_c = \sqrt{\frac{\rho}{N_T}} \mathbf{H}_c \mathbf{x}_c + \mathbf{n}_c \quad \text{or also as} \quad \mathbf{y}_c = \sqrt{\frac{E_s}{\sigma_n^2}} \mathbf{H}_c \mathbf{x}_c + \mathbf{n}_c, \tag{2.25}$$

where now the real alphabets in each dimension is

$$\mathcal{A} = \sqrt{\frac{3}{2(M-1)}} \left\{ -(\sqrt{M}-1), \cdots, -5, -3, -1, +1, +3, +5, \cdots + (\sqrt{M}-1) \right\}, \tag{2.26}$$

to assure that $E\{x_i^* x_i\} = 1$ and $E\{\mathbf{x}^H \mathbf{x}\} = N_T$.

The norms in (2.21) are the Euclidian norm. Notice that for the case of matrices several norms may be defined [148] (ch. 4). The Frobenius norm

$$\left\| \mathbf{A} \right\|_F = \sqrt{\text{trace}\left(\mathbf{A}^H \mathbf{A} \right)} = \sqrt{\text{trace}\left(\mathbf{A} \mathbf{A}^H \right)} = = \sqrt{\sum_i \sum_j \left| a_{ij}^2 \right|} \tag{2.27}$$

is the matrix norm that is adopted throughout this thesis whenever a matrix norm is necessary (mostly to define metrics of similarity for matrices). It is not difficult to see that in this norm

[12] The error rate is also sometimes given in the MIMO literature in terms of the bit error rate (BER), which is obtained from the SER taking in consideration the number of bits per complex symbol.

$$E\left\{\left\|\mathbf{H}_c\right\|_F^2\right\} = N_T N_R \,. \tag{2.28}$$

In this dissertation, the uncorrelated channel is considered, as seen in the definition of $\mathbf{H}_c$. When correlation exists between the multipath components, a more general model is necessary and that implies a full characterization of the correlation matrix involving the cumbersome vectorisation of $\mathbf{H}_c$ (see, e.g., [43] (sec. 3.1.1)). The Kronecker model is a popular way of avoiding this, by decoupling the effect of correlation at the transmit side (characterised by $\mathbf{R}_{c,\mathrm{Tx}}$) from effects at the receive side (characterised by $\mathbf{R}_{c,\mathrm{Rx}}$). Then, the model consists only of matrix multiplications[13]

$$\mathbf{H}_c = R_{c,\mathrm{Rx}}^{1/2} H_{\mathrm{c,ind}} R_{c,\mathrm{Tx}}^{1/2} \,. \tag{2.29}$$

The separation of Tx and Rx effects can be interpreted as if the multipath components at the receiver had "forgotten" about the effects of antenna coupling and scattering close to the Tx, which can be considered as separate from what happens in terms of antenna coupling and scattering close to the Rx.

For signals with *symbol time* T and *bandwidth* B, as a rule of thumb, the coherence time and the coherence bandwidth are given by:

$$B_{coh} \approx \frac{1}{\text{rms delay spread}} \quad , \quad \tau_{coh} \approx \frac{1}{\text{Doppler spread}} \,. \tag{2.30}$$

When assessing the performance of SM systems, this work will consider the channel to be i) *flat* (nonselective in the frequency domain), i.e., $B < B_{coh}$, and ii) *slow* (nonselective in time for a transmit vector), that is, $T < \tau_{coh}$. For typical values for the coherence time in different mobility scenarios in LTE see [53] (sec. 2.4). Typical descriptions of the wireless channels can be found in, e.g., [53] (sec. 2.4), [41] (sec. 1.3) and a deeper discussion is offered by [43].

[13] The square is root of a matrix defined as $\mathbf{A}^{1/2} = \mathbf{U}\Sigma^{1/2}\mathbf{V}^H$, where $\mathbf{U}$ and $\mathbf{V}$ are the unitary matrices of the SVD of $\mathbf{A}$, with Σ the diagonal matrix made of the singular values of $\mathbf{A}$ [35](p.18).

2.2.2 – The Real Equivalent Model

The model for spatial multiplexing was described in (2.17) in terms of complex vector spaces, however it is not difficult to prove that, by stacking the real and complex parts of the vectors (respectively denoted by $\Re$ and $\Im$), and by appropriate construction of a modified channel matrix, the problem can equivalently be described by means of real variables as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \Leftrightarrow \begin{bmatrix} \Re(\mathbf{y}_c) \\ \Im(\mathbf{y}_c) \end{bmatrix} = \begin{bmatrix} \Re(\mathbf{H}_c) & -\Im(\mathbf{H}_c) \\ \Im(\mathbf{H}_c) & \Re(\mathbf{H}_c) \end{bmatrix} \begin{bmatrix} \Re(\mathbf{x}_c) \\ \Im(\mathbf{x}_c) \end{bmatrix} + \begin{bmatrix} \Re(\mathbf{n}_c) \\ \Im(\mathbf{n}_c) \end{bmatrix} \tag{2.31}$$

with $\mathbf{y} = \left[y_1, y_2, \ldots, y_{2N_R} \right]^T \in \mathbb{R}^{N_R \times 1}$, $\mathbf{x} = \left[x_1, x_2, \ldots, x_{2N_T} \right]^T \in \mathbb{R}^{N_T \times 1}$, $\mathbf{n} = \left[n_1, n_2, \ldots, n_{2N_R} \right]^T \in \mathbb{R}^{N_R \times 1}$, and $\mathbf{H} \in \mathbb{R}^{N_R \times N_T}$ (notice that the "c" subscripts in the variables will be dropped from now on). Expanding (2.31), each component of $\mathbf{y}$ is

$$\begin{cases} y_i = \Re h_{i,1} \cdot \Re x_1 + \cdots + \Re h_{i,N_T} \cdot \Re x_{N_T} \\ \qquad - \Im h_{i,1} \cdot \Im x_1 - \cdots - \Im h_{i,N_T} \cdot \Im x_{N_T} + \Re n_i, \quad i \le N_R \\ y_i = \Im h_{i-N_R,1} \cdot \Re x_1 + \cdots + \Im h_{i-N_R,N_T} \cdot \Re x_{N_T} \\ \qquad + \Re h_{i-N_R,1} \cdot \Im x_1 + \cdots + \Re h_{i-N_R,N_T} \cdot \Im x_{N_T} + \Im n_{i-N_R}, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad N_R < i \le 2N_R \end{cases} \tag{2.32}$$

and therefore these components have a χ^2 distribution with $2N_T$ degrees of freedom, , before the noise is added.

The equivalent real model is the one that will be used throughout this work and therefore the transposition operator, T, will replace the Hermitian operator, H, (conjugation followed by transposition). Moreover, orthogonal matrices play the role of singular matrices, for instance in the singular value decomposition (SVD) or for performing orthogonal rotations on lattices. In this model, the discrete inputs in the elements of $\mathbf{x}$ that are considered in this dissertation are taken from the real alphabet $\mathcal{A}$, as defined in (2.19). In this model, both real and imaginary components of $\mathbf{n}_c = \Re(\mathbf{n}_c) + j\Im(\mathbf{n}_c)$ have variance

$$\sigma_n^2 = \frac{1}{2} \frac{N_T E_s}{\rho}. \tag{2.33}$$

Another consequence of this model is that, henceforth, full rank real lattices will be considered to have n dimensions.

2.2.3 – Capacity with CSIR

Assuming that there is perfect channel state information at the receiver (CSIR), i.e., perfect knowledge of $\mathbf{H}$, it can be proven that the maximization of the mutual information between the input and output in MIMO amounts to maximising $\log_2\left(\det(\pi e\mathbf{R}_y)\right)$. The output covariance is $\mathbf{R}_y = E\left\{\mathbf{y}\mathbf{y}^H\right\} = \mathbf{H}\mathbf{R}_x\mathbf{H}^H + \sigma_n^2\mathbf{I}_{N_R}$ and therefore the capacity is

$$C = \max_{\mathbf{R}_x} \log_2 \det\left(\mathbf{I} + \frac{\rho}{N_T}\mathbf{H}\mathbf{R}_x\mathbf{H}^H\right), \tag{2.34}$$

where $\text{trace}(\mathbf{R}_x) = E\{\mathbf{x}^H\mathbf{x}\} < 1$ is the transmit power constraint in the optimization problem. When the channel *is* known at the transmitter (Tx), i.e., there is CSIT, the input covariance can be built to match the channel. When CSIT does *not* exist, the input is made to have $\mathbf{R}_x = \sigma_x^2\mathbf{I}_{N_T}$, leading to a capacity

$$C = \log_2 \det\left(\mathbf{I} + \frac{\rho}{N_T}\mathbf{H}\mathbf{H}^H\right), \tag{2.35}$$

where CSIR is assumed. This implies that the receiver is able to accurately estimate the channel matrix.

The matrix $\mathbf{H}\mathbf{H}^H$ can be interpreted as the Gram matrix associated with the lattice generated by the *rows* of $\mathbf{H}$. Therefore, as shown in section 2.1.2, $\mathbf{H}\mathbf{H}^H$ is a semidefinite positive matrix with $r = \text{rank}(\mathbf{H})$ eigenvalues, whose values are $\lambda_i = s_i^2$, i.e., they are the square of corresponding r singular values s_i. Applying the singular value decomposition to $\mathbf{H}\mathbf{H}^H$, and remembering that a Gram matrix is symmetric, its left and right unitary matrices in the SVD are the same. Hence, (2.34) becomes

$$\log_2 \det\left(\mathbf{I} + \frac{\rho}{N_T}\mathbf{U}\mathbf{\Sigma}\mathbf{U}^H\right) = \log_2 \det\left(\mathbf{U}\left(\mathbf{I} + \frac{\rho}{N_T}\mathbf{\Sigma}\right)\mathbf{U}^H\right), \tag{2.36}$$

and

$$C = \sum_{k=1}^{r} \log_2 \left(1 + \frac{\rho}{N_T} \lambda_i\right). \tag{2.37}$$

As known from section 2.2.1, $\mathbf{H}$ is not deterministic but a random matrix. One should note that in the case of *slow fading* (when a codeword does not span more than one coherence period of the channel), regardless the choice of rate and coding scheme, there will always be a non-zero probability that the rate is higher than the capacity of the channel. Hence, the capacity that the channel can commit to is *zero* [45] (p.188). Even in that case, one can speak of the *instantaneous capacity* $C(\mathbf{H})$, as a function of the current channel.

This work will assume a channel with a *block fading* model (i.e., when a codeword goes through many different and independent channel instances [45] (p.199)). In this model the channel remains constant over a certain duration (the duration of a *block*), only changing from block to block. In this case, by taking the average of over many instances of the channel coefficients, a channel capacity can be obtained by applying an expectation to (2.37):

$$C_{\text{erg}} = E_{\lambda_i} \left\{ \sum_{k=1}^{r} \log_2 \left(1 + \frac{\rho}{N_T} \lambda_i\right) \right\}. \tag{2.38}$$

This expectation depends on the eigenvalues λ_i, which are independent random variables, each with a Wishart distribution [149], [43] (Apx.B), as Teletar first noted in [29]. While the number of receive antennas is not explicit in the capacity formula, its effect is hidden in the rank r of $\mathbf{H}\mathbf{H}^H$, which is

$$r = \min(N_t, N_R). \tag{2.39}$$

It is not difficult to show ([51] (pp. 148-149), [45] (sec. 8.2)) that for low SNR, using the approximation $\log_2(1+x) \approx x \log_2 e$ valid for small x, and noting that $E\{\lambda_i\} = \text{Trace}(\mathbf{H}\mathbf{H}^H)$, as seen in (2.35)-(2.36), then the capacity in (2.38) is

$$C_{erg} \approx N_R \rho \log_2 e. \tag{2.40}$$

This result shows that, for the low SNR, the number of transmit antennas does not play any role, because what is important is the fact that N_R receive antennas can

coherently combine the incoming signals working as a "spatial matched filter". This result will be revisited in Chapter 3, when both linear receivers are shown to approach the matched filter when noise is high compared to the mutual interference between layers. In the high SNR regime, it is also not difficult to conclude that expression (2.38) becomes

$$C_{\text{erg}} \approx r \log_2\left(\frac{\rho}{N_T}\right) + \sum_{i=1}^{r} E_{\lambda_i}\left\{\log_2\left(\lambda_i\right)\right\}, \tag{2.41}$$

which, remembering (2.39), shows the famous linear increase of the ergodic capacity with the minimum number of antennas on each side.

In STC a codeword spans more than one transmit vector, as a matrix assumes the role of $\mathbf{x}_c$ in the model (2.17) and several vectors may experience different channel realizations $\mathbf{H}_i$ over time. Moreover, using outer-codes the codewords may experience enough channel realisations and the average of the capacities of the channels may be close to the ergodic capacity. In the case of *uncoded* SM, those situations do not exist and therefore the outage capacity and the outage probability are the concepts best suited to describe these systems.

In 2004, Guo, Verdú and Shamai made a breakthrough in information theory, finding a very simple relation between mutual information and the minimum mean square error at a receiver. Debbah in [31] (Ch.2) shows how that approach eventually leads to a pleasing (average) geometrical interpretation for the capacity of a MIMO system, much similar to that of the traditional geometrical interpretation of capacity of the binary symmetric channel, as first observed by Shannon. The determinant of the auto-correlation matrix of the transmitted symbols measures the volume of space associated with a MIMO code word. The determinant of the covariance matrix of the MMSE estimate measures the small volume around the received vector, where the signal is expected to lie with high probability. It can be proven that the MIMO capacity is

$$C = \log_2 \frac{\det\left(\mathbf{R}_{xx}\right)}{\det\left(\mathbf{R}_{\text{MMSE}}\right)}, \tag{2.42}$$

which amounts to the *sphere packing problem* in lattices [19],[20]. It is worth noting that Stoica et al. have independently arrived at the exact same lattice interpretation solely by signal processing considerations [150].

2.3 – Detection in MIMO SM

While in STC the central research problem is finding codes that maximise the codeword pairwise distance and thus that minimises pairwise error probability (e.g., [77]), the main research problem in spatial multiplexing in the last ten years has been detecting $\mathbf{x}$ given the noisy observation $\mathbf{y}$. For that problem, the *maximum a posterior probability* (MAP) of $\mathbf{x}$ is

$$\mathbf{x} = \arg\max_{\mathbf{x}\in\mathcal{A}} P\left(\mathbf{x}\middle|\mathbf{y}\right) = \arg\max_{\mathbf{x}\in\mathcal{A}} \frac{P\left(\mathbf{x}\middle|\mathbf{y}\right)P(\mathbf{x})}{P\left(\mathbf{y}\right)} \tag{2.43}$$

As all vectors $\mathbf{x}$ are equiprobable, $P\left(\mathbf{x}\middle|\mathbf{y}\right)$ is a sufficient statistics for the detection process. Therefore, MAP detection can be reduced to *maximum likelihood* (ML) without any performance loss. For the i.i.d. Rayleigh channel with i.i.d. transmitted symbols with $\mathbf{R}_x = \sigma_x^2\mathbf{I}_n$ and $\mathbf{R}_n = \sigma_n^2\mathbf{I}_n$, one has the N-dimensional probability distribution

$$P\left(\mathbf{x}\middle|\mathbf{y}\right) = \frac{1}{\left(2\pi\sigma_n^2\right)^{N/2}}\exp\left(-\frac{(\mathbf{y}-\mathbf{H}\mathbf{x})^T(\mathbf{y}-\mathbf{H}\mathbf{x})}{2\sigma_n^2}\right) = \frac{1}{\left(2\pi\sigma_n^2\right)^{N/2}}\exp\left(-\frac{\left\|\mathbf{y}-\mathbf{H}\mathbf{x}\right\|^2}{2\sigma_n^2}\right), \tag{2.44}$$

and therefore the detection problem becomes that of minimizing the exponent of (2.44):

$$\hat{\mathbf{x}}_{ML} = \arg\max_{\mathbf{x}\in\mathcal{A}} \left\{\left\|\mathbf{y}-\mathbf{H}\mathbf{x}\right\|^2\right\}. \tag{2.45}$$

This problem now has a clear *geometrical* interpretation: the optimal $\mathbf{x}$ (the one that best explains the observation $\mathbf{y}$) is the one that, among all possible input vectors, and after the linear transformation, generates the closest vector $\mathbf{H}\mathbf{x}$ (in the Euclidian sense) to the received vector $\mathbf{y}$. This problem is known in integer optimisation as *integer least squares* and in lattice theory as CVP (as mentioned above): "given a target vector off the lattice, $\mathbf{y}$, which point in the lattice is the closest one?". The

problem is exemplified in Figure 2.6 for the simple cases of $\mathbb{Z}$, $\mathbb{Z}^2$, and $\mathbb{Z}^3$ lattices (the CVP in these lattices is not NP-hard; it will be seen in Chapter 3 that for $\mathbb{Z}^n$ lattices the algorithmic detection complexity of the optimal detector is actually polynomial $\mathcal{O}(n^3)$, due to the orthogonal structure).

The solution of the CVP is equivalent to drawing a Voronoi cell around the target point and finding which single lattice point lies inside the region. Conversely, this is equivalent to having the lattice tiled by the Voronoi region and in selecting which region the target is. Obviously, computing the Voronoi region is also NP-hard.

Notice that the complex-valued lattice in a MIMO link with N_T transmit antennas and a M-QAM modulation will have M^{N_T} complex points within its border. In the equivalent real model the number is obviously the same, $\left(\sqrt{M}\right)^{2N_T}$.

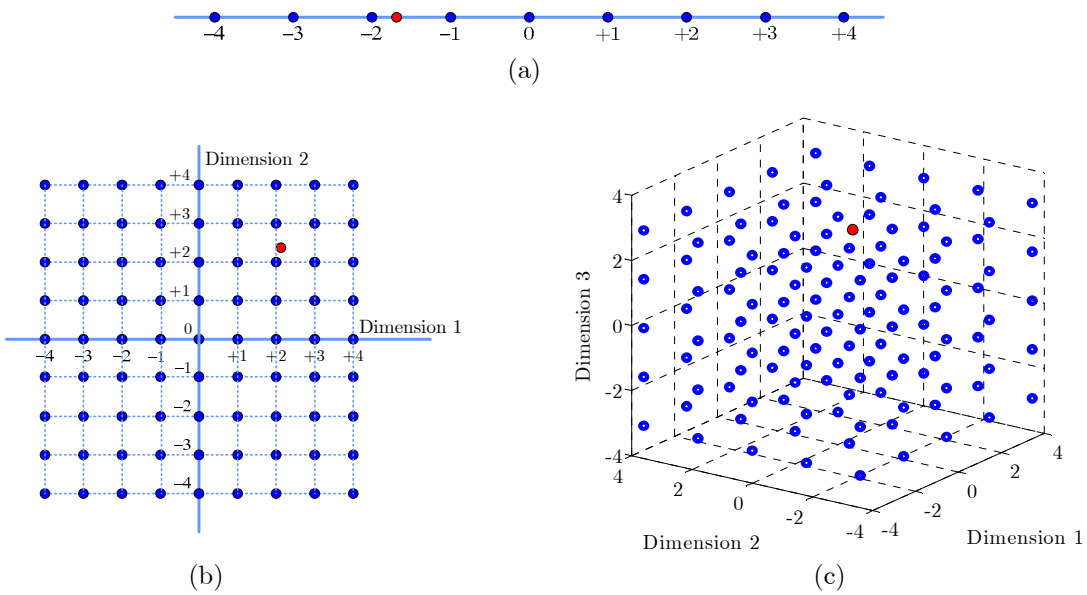


Figure 2.6: The closest vector problem in one, two and three dimensions, given an off-lattice target point.

2.3.1 – The Complexity of Optimal Detection

The algorithmic complexity of the CVP is proven to be *NP-hard*, which, in the current state of understanding of the complexity of algorithms, places it in the worst

tier in the hierarchy of complexity classes. One should not conclude from this that any hope of finding accurate solutions should be deemed unrealistic. In fact, it will be seen throughout this work that very good approximations to the optimal solution can be found, especially when the number of dimensions is small [151]. As the number of dimensions grows, the complexity of the problem, measured as the number of operations, grows exponentially (this is what is known as "the curse of dimensionality" [152]); however, the complexity of some approximate detection techniques grows only polynomially. Usually, the number of operations (flops or algebraic operations) required by an algorithm is expressed in the "big O" notation[14] and in practice this suffices for comparing the complexity of algorithms, *when* it is feasible to test them. However, the complexity theory of algorithms is a vast and convoluted topic (e.g., [153]), and the precise definition of each of the complexity classes falls beyond the scope of this work. Nonetheless, there are simpler and insightful working definitions describing these classes, e.g., [154], [155], [112] (Apx. B). The most broad complexity classes are P, NP, NP-complete and NP-hard and, according to what is known today, are related as shown in Figure 2.7 (if $\mathrm{P} \neq \mathrm{NP}$, as is believed to be the most likely case).

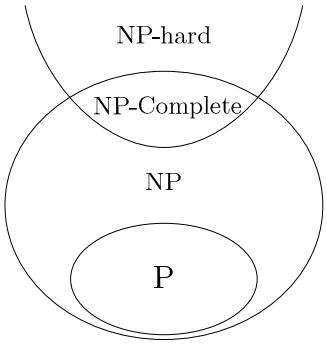


Figure 2.7: Complexity classes.

[14] For an input data of size n (e.g., n bits are necessary to represent the data, or, in the particular case of MIMO, n is the number of dimensions of the lattice), complexity $\mathcal{O}(f(n))$ means that the function $f(n)$ is an upper bound, up to a constant multiple factor, for the function of the number of operations as a function of n (a detailed description of this and other notations is given in [242]).

The P class encompasses the problems that can be solved in polynomial time (making a correspondence between the number of operations and time). NP stands for *non deterministic polynomial* complexity. It means that, if a certain *certificate* is provided (i.e., a possible "solution" to the problem), it is then possible to verify in polynomial time if that certificate is a valid solution to the problem or not. This involves a mere yes/no answer because the problem is formulated as a *decision problem*. As every problem in P can also be posed as a decision problem (one just needs to use the solution as a certificate), then $\mathrm{P} \subset \mathrm{NP}$ .The problems in the NP-complete class all share the property that if one of them is proven to be in P, then all the other problems in the class would also be in P, unless the polynomial hierarchy collapses. (It is worth mentioning that the vast majority of NP problems are in fact NP-complete). Technically, these "entanglements" are proven through a "P time" *reduction* of one problem to the other. A simple definition of the NP-hard class unavoidably ends up vague: it consists of the problems that are "at least as hard as the NP-complete ones". NP-hard problems hold some property that, if solved in "P time", would make any problem in class NP-complete to be solvable in "P time", though they cannot be included in the NP-complete family. Obviously, given the definition, all problems in the NP-complete class are also NP-hard, however there exist problems that are in the NP-hard class but not in NP-complete. A useful theorem states that: if an optimization problem has a *decision version* that is NP-complete, then the *optimization version* is NP-hard. In the CVP one can think of the following decision version: "is there a lattice point at a distance shorter than some distance d from the target point?"; given a certificate, it is trivial to compute the distance and verify that such a point exists. The optimization version is the CVP itself: "what is the point at the shortest distance from the target point?". There are thousands of NP-hard problems [112] (Apx. B), such as the subset sum problem (an example of a decision problem), the knapsack problem (a problem of combinatorial optimization [156], [112]), the binary optimization problem, the travelling salesman or the CVP.

The CVP was first proven NP-Hard by van Emde Boas in 1981, but the technicalities of that proof are considered cumbersome. In 2001 [157], Micciancio was able to show a reduction from the subset sum problem (known to be NP-hard) to a CVP in a lattice, which finally proved, in a very simple and elegant way, the NP-hardness of the CVP.

As is the case of many problems in the class NP-hard, being in this class does not mean that the problem cannot ever be solved in an optimal manner. When both the number of dimensions n and the modulation order M are low, a "brute force" approach is affordable. Furthermore, when ML-type detection is no longer possible, the challenge of finding sub-optimal affordable solutions can be quite successful. The next chapter will describe how the geometry of lattice is closely related with the detection strategies used in MIMO.

2.4 – Summary

This chapter introduced many of the definitions and concepts that will be used later on in this dissertation. The first half of this chapter described basic concepts on lattices and explained the geometric connection between a lattice and its dual. In the second part of the chapter MIMO was framed as a lattice problem and the complexity of the underlying CVP has been addressed.

Chapter 3 – Geometry and Detection in Spatial Multiplexing

As we know, lattices are good for almost everything."
Giuseppe Caire, 2007
[Question time after a talk at ISIT, Nice, France]

This chapter starts by introducing the most important type of MIMO receivers and the geometric concepts associated with them, which explain their performance loss in respect to the optimum detector. The linear receivers, which are the simplest ones, but also the ones having the worst SER, are the first ones to be geometrically interpreted. Then, the ordered successive interference cancelation (OSIC) technique is described, followed by the lattice-reduction-aided (LRA) approach, and finally the sphere-decoding concept is introduced.

The last part of this chapter capitalises on the geometric relation between primal and dual lattices and proposes a receiver, for slow fading channels, that samples some points nearby the received vector and makes them candidate solutions to the CVP. This sampling makes use of projections onto distinct families of parallel hyperplanes where the density of lattice points is maximised.

3.1 – Linear Receivers

Linear receivers consists of i) a linear transformation $\mathbf{W}$ of the received vector which then followed by ii) a quantisation to the symbol alphabet (also known as *slicing*). The linear transformation is a filter that can be designed with two different criteria, leading to the *zero-forcing* (ZF) detector or to the *minimum mean square error* (MMSE) detector. These receivers constitute the simplest set of (non optimal) receivers to be widely used for MIMO receivers. The detected solution $\hat{\mathbf{x}}$ given by these techniques is obtained by applying

$$\mathbf{x}_W = \mathbf{W}\mathbf{y}\,, \tag{3.1}$$

$$\hat{\mathbf{x}}_W = Q_{\mathbb{Z}}\left[\mathbf{x}_W\right], \tag{3.2}$$

where $Q_{\mathbb{Z}}[\cdot]$ denotes rounding to the nearest integer and the subscript W in $\hat{\mathbf{x}}_W$ indicates the filter design criterion: ZF or MMSE.

D-BLAST was the first technique to be proposed [28], followed by the more practical OSIC [85], but, as will be seen below, OSIC includes a linear inversion (either ZF or MMSE). As mentioned in section 1.2.3, both ZF and MMSE techniques are well known in other contexts of detection and equalisation in SISO (c.f. Table 1.2), but the formalism that is used in MIMO is the one that was first developed for multiuser detection [87].

In both types of linear receivers the linear transformation $\mathbf{W}$ can be seen as a focusing process of the points in the received lattice back onto $\mathbb{Z}^n$ (or $\mathbb{C}^n$). This "backwards transformation" is of interest because it maps the received lattice back onto $\mathbb{Z}^n$, which lends itself to simple orthogonal *slicing*. This is the primary motivation for this particular design. In 0 the concept of a having a linear transformation as the first stage of a detection technique will be generalised to the concept of *focusing* a received lattice onto some other given lattice, whose geometric structure is also of interest.

Noticeably, despite the early use of both ZF and MMSE detectors, a thorough theoretical understanding of their performance seems not to have been pursued until very recently [84].

3.1.1 – Zero-forcing Detection

It is natural to think first of a solution to (2.45) involving the linear transformation that *undoes* the linear transformation, which is obviously the inverse matrix.

The inversion of $\mathbf{H}$ is a trivial operation (e.g., by applying Gauss elimination to an extended matrix), but can only be defined for matrices with non-zero determinant (i.e., *invertible* or *non-singular* matrices). Hence the need for $N_T < N_R$. A geometrical interpretation for the cases with singular matrices is simple. A *singular* matrix that defines a lattice in $\mathbb{R}^n$ (the extension to $\mathbb{C}^n$ is always implied) performs a linear transformation whose outcome is a "flat" lattice that lies on a "flat subspace" of that space, that is, a lattice that does not fill all the dimensions in $\mathbb{R}^n$ and consequently can be fully described in a smaller dimensional space. For example, think of lattices that lie on a 2D plane or on a straight line embedded in an n-dimensional real space. In the space in which they are defined, these lattices have zero volume (i.e., zero determinant). Even so, an inverse correspondence to the original lattice seems still impossible. This would only not be possible if $N_R < N_T$, since the higher dimensional transmit lattice in N_T cannot, in general, be captured in a lower dimensional space.

The algebraic interpretation of the channel inversion problem of an $n \times n$ singular channel matrix $\mathbf{H}$ is related to its *singular value decomposition* $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T$, where $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices and $\mathbf{\Sigma} = \text{diag}\left(\lambda_1, \lambda_2, \cdots, \lambda_r\right)$, the diagonal matrix with the singular values of $\mathbf{H}$. The inverse is $\mathbf{H} = (\mathbf{V}^T)^{-1}\mathbf{\Sigma}^{-1}\mathbf{U}^{-1}$, or $\mathbf{H} = \mathbf{V}\mathbf{\Sigma}^{-1}\mathbf{U}^T$, as both $\mathbf{U}$ and $\mathbf{V}$ are unitary. Since the inverse of the diagonal matrix is $\mathbf{\Sigma} = \text{diag}\left(1/\lambda_1, 1/\lambda_2, \cdots, 1/\lambda_r\right)$, when there are only $r < n$ non-zero singular values (i.e., the rank is r), then $n - r$ singular values cannot be inverted in a finite domain.

The *pseudo-inverse* matrix, also known as the *Moore-Penrose*[15] *(inverse) matrix*, is the solution to the *normal equation* $\mathbf{H}^H\mathbf{y} = \mathbf{H}^H\mathbf{H}\mathbf{x}$, obtained from (2.31). The straightforward solution to this equation is to make $(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\mathbf{y} = \mathbf{x}$, where $\mathbf{H}^H\mathbf{H}$ is invertible because it is positive definite (indeed, it corresponds to the Gram matrix of the lattice). The Moore-Penrose inverse of $\mathbf{H} \in \mathbb{C}^{N_R \times N_T}$, when $N_R > N_T$, *always* exists and is defined as

$$\mathbf{H}^+ = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H . \tag{3.3}$$

From (3.1) and (3.2), the ZF receiver is, formed by the pseudo-inverse matrix (the linear filter) followed by a quantisation to the symbol alphabet by threshold decision, i.e.,

$$\mathbf{W}_{ZF} = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H \quad , \quad \mathbf{x}_{ZF} = \mathbf{W}_{ZF}\mathbf{y} \quad , \quad \hat{\mathbf{x}}_{ZF} = Q_{\mathcal{A}}\left[\mathbf{x}_{ZF}\right] \tag{3.4}$$

and therefore

$$\hat{\mathbf{x}}_{ZF} = Q_{\mathcal{A}}\left[\mathbf{W}_{ZF}(\mathbf{H}\mathbf{x} + \mathbf{n})\right] = Q_{\mathcal{A}}\left[\mathbf{x} + \mathbf{W}_{ZF}\mathbf{n}\right]. \tag{3.5}$$

The filtered noise is transformed by $W_{ZF} = \mathbf{H}^+$, which constitutes a noise enhancement factor. The receiver structure is shown in Figure 3.1.

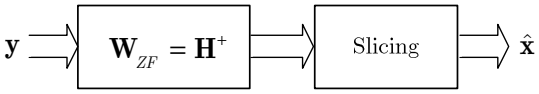


Figure 3.1: Zero-forcing receiver.

The detected vector $\hat{\mathbf{x}}_{ZF}$, as obtained from (3.5), is in fact the solution to

$$\hat{\mathbf{x}}_{ZF} = \underset{\mathbf{x}\in\mathbb{C}^{N_T}}{\arg\min}\left\{\left\|\mathbf{y} - \mathbf{H}\mathbf{x}\right\|\right\}. \tag{3.6}$$

Comparing (3.6) with (2.45) one should note how the search is now made in the *continuous* domain $\mathbb{R}^n$ (or in $\mathbb{C}^n$, for complex lattices) instead of the discrete complex

[15] Discovered first by E. H. Moore in 1920 and later re-discovered by Roger Penrose in 1955 (published in the Proceedings of the Cambridge Philosophical Society, vol. 51, pp. 406-413, 1955).

alphabet $\mathcal{A}$ (or $\mathcal{A}_c$). This is the origin of the sub-optimality of the ZF receiver. As mentioned previously after the inverse transformation, all the points in the lattice are matched to the initial $\mathbb{Z}^n$. The orthogonal geometry of $\mathbb{Z}^n$ eliminates all the interference between the dimensions of the lattice, i.e., between the MIMO layers; in a system with $N_T = N_R$, the i^{th} antenna at the receiver "sees" the transmission from the corresponding i^{th} antenna at the transmitter cleared from any interference from the other $N_T - 1$ antennas. If $N_T < N_R$ the same happens in the appropriate sub-dimensions of $\mathbf{y}$. The name zero-forcing is due to the fact that the interference in each antenna is *forced to zero*. In a Euclidian signal space, the geometrical interpretation is that ZF projects the received vector onto the space that is orthogonal to space where all the interferers lie (as illustrated in Figure 3.2).

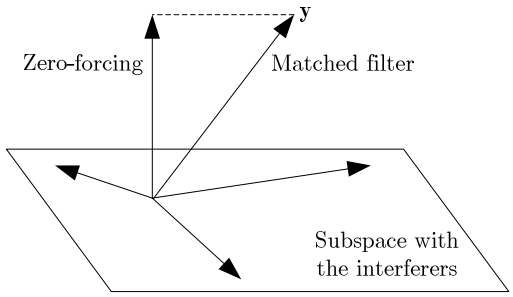


Figure 3.2: Geometric interpretation of ZF filtering in a signal space.

This generalised pseudo-inverse transformation for singular matrices holds properties that are similar to the properties of the "true" inverse matrix of a non-singular matrix (for an extensive description of the properties see [158] (sec. 4.4)).

Any solution to (2.45) involving the inversion of $\mathbf{H}$ will imply a number of operations that depends on the inversion methods used. The number of those operations is given in [158] (p. 170) and are listed in Table 3.1. The common assumption in MIMO literature is that the number of operations involved in ZF (or in any stage involving channel inversion) is $\mathcal{O}(n^3)$ and Table 3.1 corroborates that this is the case for all the inversion methods listed.

Table 3.1: Number of operations involved in solving $\mathbf{y} = \mathbf{Hx}$ by several methods based on channel inversion (with a square $\mathbf{H}$).

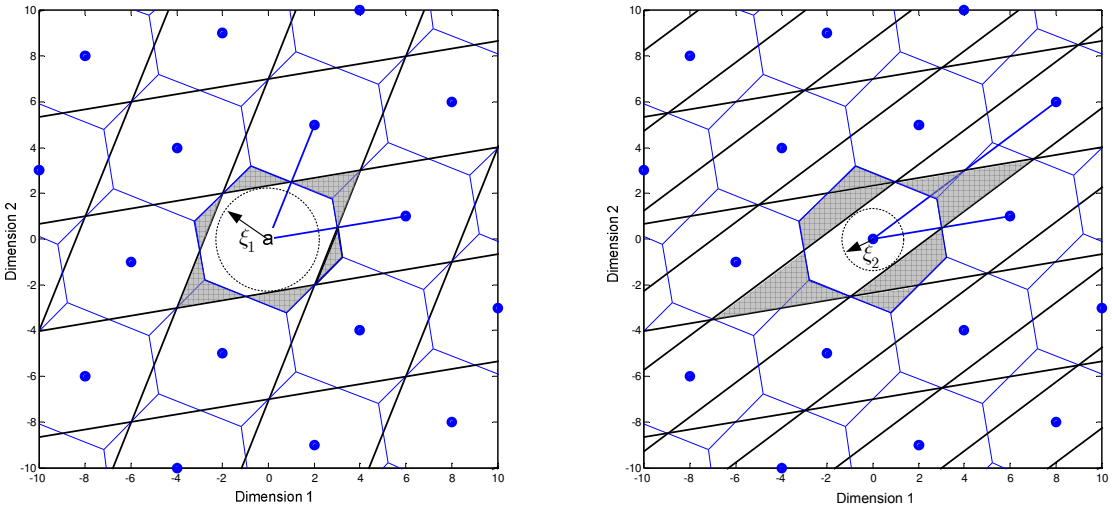
	Additions and subtractions	Multiplications and divisions
Gauss elimination with back substitution	$\frac{1}{3}n^3 + \frac{1}{2}n^2 - \frac{5}{6}n$	$\frac{1}{3}n^3 + n^2 - \frac{1}{3}n$
Gauss-Jordan elimination (reduced Echelon form)	$\frac{1}{3}n^3 + \frac{1}{2}n^2 - \frac{5}{6}n$	$\frac{1}{3}n^3 + n^2 - \frac{1}{3}n$
Cramer's rule[159]	$(n+1)!$	$(n+1)!$
Inversion of $\mathbf{H}$, when it is non-singular	$n^3 - n^2$	$n^3 + n^2$

3.1.2 – The Geometry of ZF Detection

As is mentioned in the previous section, ZF solves the CVP by relaxing it to a search in a continuous neighbourhood instead of computing the distance between the received vector (also called the *target*) and every point in the lattice. The geometrical implication can be better understood thinking of the linear transformation of the hypercubic Voronoi regions of $\mathbb{Z}^n$ by $\mathbf{H}$. The resulting regions are called the *ZF decision regions* and correspond to the space where a lattice point will be interpreted as being close to the lattice point associated with that region.

The decision regions associated with ZF criterion are simple to obtain as they are the fundamental region $\mathcal{R}(\mathbf{H})$, as defined in (2.2). Because the lattices in MIMO are the Gaussian lattices defined in section 2.2.1, the basis generated by a channel may have some highly correlated vectors. Geometrically, this corresponds to lattices with very narrow fundamental regions, which are generated by ill-conditioned matrices, i.e., when one or more singular values are close to zero, and consequently the volume of the lattice vanishes. Figure 3.3 shows the ZF decision regions associated with the following equivalent bases:

$$\mathbf{H}_1 = \begin{bmatrix} 6 & 2 \\ 1 & 5 \end{bmatrix} \quad \text{and} \quad \mathbf{H}_2 = \begin{bmatrix} 6 & 8 \\ 1 & 6 \end{bmatrix}. \tag{3.7}$$



(a) $\mathbf{H}_1$. (b) $\mathbf{H}_2$.

Figure 3.3: Decision regions associated with the two different bases of the same lattice.

Let us concentrate in the case where the transmit point was the origin. The shaded areas indicate regions which will lead to wrong decisions when using the ZF technique: either because the point is inside the Voronoi region and outside the ZF decision region or because the closest lattice point would be decided as being the origin while the Voronoi region shows that to be false. It is possible to observe in Figure 3.3 that different bases will output different decisions given a target point. For the examples at a given SNR, the SER with $\mathbf{H}_1$ will be always lower, because the *coverage* of the MLD (i.e., Voronoi) regions is larger than in the case of basis $\mathbf{H}_2$. The notion of coverage is essential to understand MIMO detection [147]. In order to simplify the operational meaning of coverage, Ling [160] introduced the notion of *proximity factors* dependent on the notion of the largest sphere that can be fitted inside the region of coverage. These spheres are also shown in Figure 3.3 for the two basis, having *decoding radii* ξ_1 and ξ_2 respectively.

A receiver with a better performance is the one whose decision regions better approximate the shape of the regions associated with MLD. The receiver to be

presented in Chapter 6 aims to maximise this matching between its decision regions and the ones of MLD.

3.1.3 – Algebraic Analysis of ZF

It is also possible to explain the behaviour of ZF analytically. One starts by noticing that the covariance matrix of the noise affecting the decisions after any linear transformation $\mathbf{W}$ is (for complex lattices)

$$\begin{aligned}\mathbf{R}_{n,\mathbf{W}} &= E\left\{(\mathbf{Wn})(\mathbf{Wn})^H\right\} = E\left\{\mathbf{Wnn}^H\mathbf{W}^H\right\} \\ &= \mathbf{W}\mathbf{R}_n\mathbf{W}^H.\end{aligned} \tag{3.8}$$

The output SNR of ZF detected vector (before slicing) at the i^{th} layer is

$$\rho_{ZF,i} = \left[\frac{\mathbf{R}_x}{\mathbf{R}_{n,ZF}}\right]_{i,i} = \left[\frac{\sigma_x^2\mathbf{I}}{\mathbf{W}_{ZF}\mathbf{R}_n\mathbf{W}_{ZF}^H}\right]_{i,i} \quad , \quad 1 \le i \le n\,. \tag{3.9}$$

For $\mathbf{W}_{ZF}$ given by (3.3) and for the model with $\mathbf{R}_x = \sigma_x^2\mathbf{I}$ and with $\mathbf{R}_n = \sigma_n^2\mathbf{I}$, this SNR becomes

$$\begin{aligned}\rho_{ZF,i} &= \frac{1}{\left[(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\left((\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\right)^H\right]_{i,i}}\rho_a = \frac{1}{\left[(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\mathbf{H}\left((\mathbf{H}^H\mathbf{H})^{-1}\right)^H\right]_{i,i}}\rho_a \\ &= \frac{1}{\left[(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\mathbf{H}\left(\mathbf{H}^{-1}(\mathbf{H}^H)^{-1}\right)^H\right]_{i,i}}\rho_a = \frac{1}{\left[(\mathbf{H}^H\mathbf{H})^{-1}\underbrace{\mathbf{H}^H\underbrace{\mathbf{H}\mathbf{H}^{-1}}_{\mathbf{I}}(\mathbf{H}^H)^{-1}}_{\mathbf{I}}\right]_{i,i}}\rho_a \\ &= \frac{1}{\left[(\mathbf{H}^H\mathbf{H})^{-1}\right]_{i,i}}\rho_a \quad , \quad 1 \le i \le n.\end{aligned} \tag{3.10}$$

This expression relates the input SNR per transmit antenna with the output SNR at each receive antenna and quantifies the noise enhancement that explains the poor performance of ZF detection when deciding for $\hat{\mathbf{x}}_{ZF}$. One may note in (3.10) that the denominator $(\mathbf{H}^H\mathbf{H})^{-1}$ is the inverse of the Gram matrix $\mathbf{G}$, i.e., is the Gram matrix of the dual lattice, according to (2.15). When this Gram matrix is close to the identity

matrix, that means the lattice is generated by some unitary matrix $\mathbf{U}$ (orthonormal in the real model), with $\mathbf{U}\mathbf{U}^H = \mathbf{U}^H\mathbf{U} = \mathbf{I}$. In this case, the interference between all layers is zero, and no noise enhancement will happen in ZF detection. However, when the lattice is not orthogonal, $\left[(\mathbf{H}^H\mathbf{H})^{-1}\right]_{i,i} = \mathbf{G}_{ii}^{(D)}$ corresponds to the quadratic norm of the generators of the dual vector. According to the interpretation given in section 2.1.3, when these generators of the dual are large, the lattice will have a narrow separation between the parallel hyperplanes where the lattice points lie, and so have a small decoding radius. This brings together the algebraic analysis and the geometrical interpretation.

The diversity order collected by the ZF is $N_R - N_T + 1$, as known since the early papers on MIMO. The analytical proof of that was later given by Ma and Zhang in [161]

3.1.4 – Minimum Mean Squared Error Detection

The other (and more sophisticated) linear receiver aims at finding the filter that minimises the mean squared error between the estimated vector and the original vector, i.e., the filter should be

$$\mathbf{W}_{MMSE} = \arg\min_{\mathbf{W}} E\left\{\left\|\mathbf{W}\mathbf{y} - \mathbf{x}\right\|^2\right\}. \tag{3.11}$$

This criterion does not aim at cancelling all the interference between layers as does ZF. Instead, the MMSE criterion takes into consideration both the interference *and* the noise in order to minimise the expected error. This minimization implies finding the point where the gradient of the objective function in (3.11) is zero. There is however a fast track to finding this estimator by applying the *orthogonality principle*, well known in estimation theory and widely used in equalisation problems in the ISI channel [94] (secs. 2.2.3, 2.3.4), [162] (sec. 5.2), [163] (sec. 5.6)[16]. The optimum estimator for (3.11)

[16] The principle is valid for in general estimation theory and can be derived in a Bayesian framework for linear estimation, [164] (ch. 12), [250] (Secs. V-C, VII-C1).

is the one that produces an error vector $\Delta = \mathbf{W}_{MMSE}\mathbf{y} - \mathbf{x}$ that is orthogonal to received signal, i.e., the two vectors are uncorrelated (as illustrated in Figure 3.4).

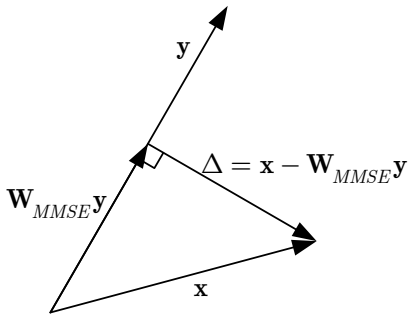


Figure 3.4: Orthogonality principle: the expected error is made orthogonal between the receive vector and the space where the best solution is searched.

The minimum norm $\|\Delta\|$ occurs when $\mathbf{W}_{MMSE}\mathbf{y} \perp \Delta$, that is

$$E\left\{(\mathbf{W}_{MMSE}\mathbf{y} - \mathbf{x})\mathbf{y}^H\right\} = 0\,. \tag{3.12}$$

Applying this principle, $\mathbf{W}_{MMSE}$ can be obtained from (using complex vectors)

$$\begin{aligned} & \mathbf{W}_{MMSE}E\left\{\mathbf{y}\mathbf{y}^H\right\} - E\left\{\mathbf{x}\mathbf{y}^H\right\} = 0 \\ \Leftrightarrow\ & \mathbf{W}_{MMSE}\left(\mathbf{H}\mathbf{R}_x\mathbf{H}^H + \mathbf{R}_n\right) - E\left\{\mathbf{x}(\mathbf{H}\mathbf{x})^H\right\} = 0 \\ \Leftrightarrow\ & \mathbf{W}_{MMSE}\left(\mathbf{R}_n + \mathbf{H}\mathbf{R}_x\mathbf{H}^H\right) - \mathbf{R}_x\mathbf{H}^H = 0 \\ \Leftrightarrow\ & \mathbf{W}_{MMSE} = \mathbf{R}_x\mathbf{H}^H\left(\mathbf{R}_n + \mathbf{H}\mathbf{R}_x\mathbf{H}^H\right)^{-1}. \end{aligned} \tag{3.13}$$

At this point most authors commonly invoke the *matrix inversion lemma*[17] [164] (p. 571), [162] (pp. 565-566), and immediately obtain from it one of the two possible formulas of the MMMSE filter. That path is cumbersome and eventually ends with an expression for $\mathbf{W}_{MMSE}$ that is not even the expression that is concluded from that derivation (although it will be proven later on that they are equivalent). In the following is presented a derivation of the filter involving much simpler algebra[18]:

[17] The matrix inversion lemma states, $\left(\mathbf{A}+\mathbf{BCD}\right)^{-1} = \mathbf{A}^{-1} - \mathbf{A}^{-1}\mathbf{B}(\mathbf{D}\mathbf{A}^{-1}\mathbf{C}^{-1})^{-1}\mathbf{D}\mathbf{A}^{-1}$, is actually one of the several variants of the Woodbury's identity [243] (p.17). Moreover, the lemma is a particular case of the Hendersson-Searle formulas [158] (sec. 1.2.1).

[18] The steps taken here are mostly used when proving several of the Hendersson-Searle formulas.

$$\begin{aligned}\mathbf{W}_{MMSE} &= \mathbf{R}_x\mathbf{H}^H\left(\mathbf{R}_n + \mathbf{H}\mathbf{R}_x\mathbf{H}^H\right)^{-1} \\ &= \mathbf{R}_x\mathbf{H}^H\left(\mathbf{R}_n(\mathbf{I} + \mathbf{R}_n^{-1}\mathbf{H}\mathbf{R}_x\mathbf{H}^H)\right)^{-1} \\ &= \mathbf{R}_x\mathbf{H}^H\left((\mathbf{I} + \mathbf{R}_n^{-1}\mathbf{H}\mathbf{R}_x\mathbf{H}^H)^{-1}\mathbf{R}_n^{-1}\right)\end{aligned} \tag{3.14}$$

For the correlation models that were considered, (3.14) is reduced to

$$\begin{aligned}\mathbf{W}_{MMSE} &= \sigma_x^2\mathbf{I}\cdot\mathbf{H}^H\left(\sigma_n^2\mathbf{I} + \mathbf{H}\cdot\sigma_x^2\cdot\mathbf{I}\cdot\mathbf{H}^H\right)^{-1} \\ &= \mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H + \frac{\sigma_n^2}{\sigma_x^2}\mathbf{I}\right)^{-1} = \mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H + \frac{1}{\rho}\mathbf{I}\right)^{-1}\end{aligned} \tag{3.15}$$

It should be highlighted that the final expression in (3.15) is *not* the only one that appears in the literature. Just as often, one may encounter the following distinct version for the MMSE filter:

$$\mathbf{W}_{MMSE} = \left(\mathbf{H}^H\mathbf{H} + \frac{1}{\rho}\mathbf{I}\right)^{-1}\mathbf{H}^H. \tag{3.16}$$

Expressions (3.15) and (3.16) are equivalent, although this is rarely mentioned in the literature. The equivalence is a consequence of the following matrix identity:

Theorem: $(\mathbf{AB}+\mathbf{I})^{-1}\mathbf{A} = \mathbf{A}(\mathbf{BA}+\mathbf{I})^{-1}$.

Proof: The identity[19] $\mathbf{A}(\mathbf{BA}+\mathbf{I}) = (\mathbf{AB}+\mathbf{I})\mathbf{A}$ holds because

$$\begin{aligned}&\mathbf{A}(\mathbf{BA}+\mathbf{I}) = \mathbf{ABA}+\mathbf{A} = (\mathbf{AB}+\mathbf{I})\mathbf{A} \\ &\Leftrightarrow \mathbf{A}(\mathbf{BA}+\mathbf{I})\underbrace{(\mathbf{BA}+\mathbf{I})}_{\text{new term}} = (\mathbf{AB}+\mathbf{I})\mathbf{A}\underbrace{(\mathbf{BA}+\mathbf{I})}_{\text{new term}} \\ &\Leftrightarrow \mathbf{A} = (\mathbf{AB}+\mathbf{I})\mathbf{A}(\mathbf{BA}+\mathbf{I})(\mathbf{BA}+\mathbf{I})^{-1}(\mathbf{BA}+\mathbf{I})^{-1} \\ &\Leftrightarrow \underbrace{(\mathbf{AB}+\mathbf{I})^{-1}}_{\text{new}}\mathbf{A} = \underbrace{(\mathbf{AB}+\mathbf{I})^{-1}}_{\text{new}}(\mathbf{AB}+\mathbf{I})\mathbf{A}(\mathbf{BA}+\mathbf{I})^{-1} \\ &\Leftrightarrow (\mathbf{AB}+\mathbf{I})^{-1}\mathbf{A} = \mathbf{A}(\mathbf{BA}+\mathbf{I})^{-1} \qquad \blacksquare\end{aligned} \tag{3.17}$$

Similarly to (3.4), the filtering matrix $\mathbf{W}_{MMSE}$ is given by (3.15) or by (3.16)[20], and so the MMSE receiver can be described by:

[19] This identity can be seen as a particular case of one of the Searle identities [243] (p.18).

$$\mathbf{x}_{MMSE} = \mathbf{W}_{MMSE}\mathbf{y} \quad , \quad \hat{\mathbf{x}}_{MMSE} = Q\left[\mathbf{x}_{MMSE}\right], \tag{3.18}$$

with the block diagram as the one in Figure 3.5.

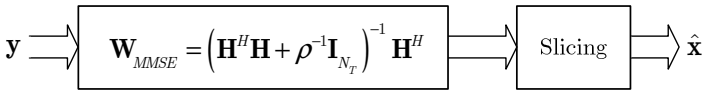


Figure 3.5: MMSE receiver.

It should be mentioned that, as shown by Hassibi in [165], (3.18) is in fact equivalent to (3.4) if $\mathbf{H}$ is replaced by the extended matrix

$$\tilde{\mathbf{H}} = \begin{bmatrix} \mathbf{H} \\ \sigma_n^2\mathbf{I} \end{bmatrix}. \tag{3.19}$$

As it is often mentioned in the literature, a careful comparison of (3.15) or (3.16) with (3.4), allows one to conclude that the MMSE filter tends to the ZF filter at high SNR. Therefore, one could expect a similar performance for both of them in the high SNR regime. However, it is well known (from very early on) that this is *not* true and this fact seems to be forgotten whenever such comment is made. It was only in 2011 that the existing gap between ZF and MMSE detection was characterised in [84]. The authors finally proved (for the ideal Rayleigh channel) several other assertions taken for granted in the last decade for the ZF, MMSE and SIC receivers based on ZF or MMSE filters. Furthermore, analytical expressions for the BER for the correlated channel have been devised in [166]. In [167] the MMSE receiver had already been analytically studied but only for low number of antennas (and also for the ideal Rayleigh fading channel).

For low SNR the effect of interference is *less* important than the effect of the Gaussian noise, hence the MMSE filter tends to $\mathbf{H}^H$, which corresponds to the *matched filter* to that channel. In this case the detection is treated as a maximum correlation problem.

---

[20] The simulations for the performance of the MMSE receivers to be presented in this dissertation all make use of (3.16) adapted for the real equivalent model (or directly applied to the complex model, in the case of Chapter 4).

The covariance matrix of the noise after the MMSE transformation is

$$\mathbf{R}_{n,MMSE} = \mathbf{W}_{MMSE}\mathbf{R}_n\mathbf{W}_{MMSE}^H , \tag{3.20}$$

and, similarly to (3.8)-(3.10),

$$\begin{aligned}\mathbf{R}_{n,MMSE} &= E\left\{(\mathbf{W}_{MMSE}\mathbf{n})(\mathbf{W}_{MMSE}\mathbf{n})^H\right\} = \\ &= E\left\{\left((\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1}\mathbf{H}^H\mathbf{n}\right)\left((\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1}\mathbf{H}^H\mathbf{n}\right)^H\right\} \\ &= E\left\{(\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1}\mathbf{H}^H\mathbf{n}\mathbf{n}^H\mathbf{H}(\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1})^H\right\} \\ &= E\left\{(\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1}\mathbf{H}^H\mathbf{n}\mathbf{n}^H\mathbf{H}(\mathbf{H}^H\mathbf{H}+\rho^{-1}\mathbf{I})^{-1})^H\right\}.\end{aligned} \tag{3.21}$$

It is possible to show that the output SNRs at the i^{th} layer after the MMSE filter becomes

$$\rho_{MMSE,i} = \frac{1}{\left[\left(\mathbf{H}^H\mathbf{H}+\rho_a^{-1}\mathbf{I}\right)^{-1}\right]_{i,i}}\rho_a \quad , \quad 1 \le i \le n\,. \tag{3.22}$$

It was seen before that the detection based in ZF is extremely problematic when its decision regions become too long and narrow. This happens for channels that are ill conditioned, with one or several of the eigenvalues very small in comparison to the others. This means that the (hyper-) ellipse associated with the linear transformation of an (hyper-) sphere is highly eccentric. In these cases one may consider penalising the solutions to the problem that would imply large a norm for the detected $\hat{\mathbf{x}}$. One other way of interpreting the MMME solution is in the context of the optimization problem generated from a relaxation of (2.45). Following the proposal of Jaldén and Ottersten in [168], one may generalise the problem for binary symbols, to the problem with $\sqrt{M}$ symbols per dimension. In doing this, the problem becomes equivalent to

$$\mathbf{y}_{MMSE} = \arg\min_{\mathbf{x}\in\mathcal{A}}\left\{\left\|\mathbf{y}-\mathbf{H}\mathbf{x}\right\|^2 + \frac{1}{\rho_a}\left\|\mathbf{x}\right\|^2 - \frac{N_T E_s}{\rho_a}\right\}, \tag{3.23}$$

noting that for $\mathbf{x} \in \mathcal{A} \Rightarrow E\left\{\rho_a^{-1}\left\|\mathbf{x}\right\|^2 - \rho_a^{-1}(N_T E_s)\right\} = 0$. The MMSE criterion in (3.23) is attained by relaxing the search in $\mathbf{x} \in A$ to a search in the continuous space where $\mathbf{x} \in \mathbb{C}^n$. As the last term in (3.23) does not involve $\mathbf{x}$, the minimisation is also

$$\mathbf{y}_{MMSE} = \arg\min_{\mathbf{x}\in\mathbb{C}^n}\{\underbrace{\left\|\mathbf{y}-\mathbf{H}\mathbf{x}\right\|^2}_{\substack{\text{(Squared) Euclidean}\\ \text{distance}}} + \underbrace{\sigma_n^2\left\|\mathbf{x}\right\|^2}_{\substack{\text{penalisation}\\ \text{on longer}\\ \text{solutions}}}\}, \tag{3.24}$$

corresponding to the solution of the typical CVP but with a term that penalises large $\left\|\mathbf{x}\right\|$ and is proportional to the energy of the the noise. This explains why MMSE performs better than ZF for ill-conditioned channel realizations.

3.1.5 – Projection Matrices

Denoting $\mathbf{H}_{\bar{j}}$ as the matrix obtained from $\mathbf{H}$ by deleting the (column) generator $\mathbf{h}_j$, it is indicated in [84] that (3.10) can also be written as

$$\begin{aligned}\rho_{ZF,j} &= \left[\mathbf{h}_j^H\mathbf{h}_j - \mathbf{h}_j^H\mathbf{H}_{\bar{j}}(\mathbf{H}_{\bar{j}}^H\mathbf{H}_{\bar{j}})^{-1}\mathbf{H}_{\bar{j}}^H\mathbf{h}_j\right]\rho_a \\ &= \mathbf{h}_j^H\left((\mathbf{I}-\mathbf{H}_{\bar{j}}\left(\mathbf{H}_{\bar{j}}^H\mathbf{H}_{\bar{j}}\right)^{-1}\mathbf{H}_{\bar{j}}^H\right)\mathbf{h}_j\rho_a \\ &= (\mathbf{h}_j^H\mathbf{P}_{\mathbf{H}_{\bar{j}}^\perp}\mathbf{h}_j)\rho_a.\end{aligned} \tag{3.25}$$

This expression can be better interpreted evoking the notion of *projection matrices*. A projection matrix is always i) symmetric, ii) idempotent (i.e., the successive application of a projection twice or more times, does not change the result), iii) positive semidefinite (e.g., [139] (p.386)).

Consider a linear space spanned by the columns of $\mathbf{H}$, i.e., span($\mathbf{H}$). The projection of a vector $\mathbf{a}$ onto that space is denoted as $\text{Proj}_{\mathbf{H}}(\mathbf{a})$, the projection onto the space orthogonal to span($\mathbf{H}$) is denoted as $\text{Proj}_{\mathbf{H}^\perp}(\mathbf{a})$, and they are given by [158] (sec. 8.3)

$$\text{Proj}_{\mathbf{H}}(\mathbf{a}) = \mathbf{P}_{\mathbf{H}}\mathbf{a} = \mathbf{H}\mathbf{H}^+\mathbf{a}, \tag{3.26}$$

$$\text{Proj}_{\mathbf{H}^\perp}(\mathbf{a}) = \mathbf{P}_{\mathbf{H}^\perp}\mathbf{a} = (\mathbf{I}-\mathbf{H}\mathbf{H}^+)\mathbf{a}. \tag{3.27}$$

From (3.26) and (3.27), the projection onto the span($\mathbf{H}_{\bar{j}}$) is

$$\mathbf{P}_{\mathbf{H}_{\bar{j}}} = \mathbf{H}_{\bar{j}}\mathbf{H}_{\bar{j}}^{+} \tag{3.28}$$

and the projection onto its orthogonal complement is

$$\begin{aligned}\mathbf{P}_{\mathbf{H}_{\bar{j}}^{\perp}} &= \mathbf{I} - \mathbf{H}_{\bar{j}}\mathbf{H}_{\bar{j}}^{+} \\ &= \mathbf{I} - \mathbf{H}_{\bar{j}}\left(\mathbf{H}_{\bar{j}}^{H}\mathbf{H}_{\bar{j}}\right)^{-1}\mathbf{H}_{\bar{j}}^{H}\end{aligned} \tag{3.29}$$

where the Moore-Penrose pseudo-inverse was used in the last line.

The factor $\mathbf{h}_j^H\mathbf{P}_{\mathbf{H}_{\bar{j}}^{\perp}}\mathbf{h}_j$ that appears in (3.25) is a quadratic form, as defined in **(2.5)**, hence, $\mathbf{h}_j^H\mathbf{P}_{\mathbf{H}_{\bar{j}}^{\perp}}\mathbf{h}_j \geq 0$ as it corresponds to the norm of the projection of generator $\mathbf{h}_j$ onto space spanned by the remaining generators in the basis $\mathbf{H}_{\bar{j}}$.

Figure 3.6 shows the geometry of these projections in the same bidimensional example of Figure 3.3, with basis $\mathbf{H}_2$, given in (3.7). One can observe that the factor $\mathbf{h}_j^H\mathbf{P}_{\mathbf{H}_{\bar{j}}^{\perp}}\mathbf{h}_j$ corresponds to the distance between parallel layers where the lattice points lie and it measures the separation between the decision thresholds for the j^{th} layer, associated with $\mathbf{h}_j$. When that distance is ≥ 1, there is a SNR gain in that layer in respect to the SNR in the expected average layer.

It is worth mentioning that in the case with ZF, $\mathbf{h}_j^H\mathbf{P}_{\mathbf{H}_{\bar{j}}^{\perp}}\mathbf{h}_j$ has a χ^2 distribution with $2(N_R - N + 1)$ degrees of freedom [84]. A similar expression to (3.25) can be obtained for MMSE if the factor $\left(\mathbf{H}_{\bar{j}}^H\mathbf{H}_{\bar{j}}\right)^{-1}$ is replaces by $\left(\mathbf{H}_{\bar{j}}^H\mathbf{H}_{\bar{j}} + \rho^{-1}\mathbf{I}\right)^{-1}$ in (3.25).

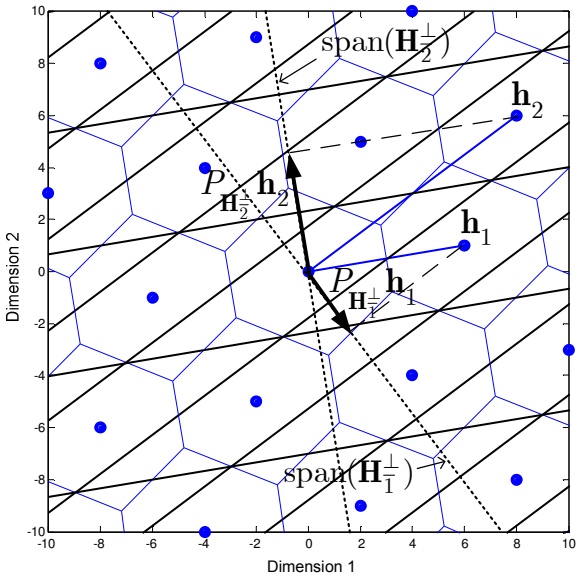


Figure 3.6: Geometry of the SNR relation factor in (3.25). Includes the Voronoi regions and the ZF decision regions of the lattice $\Lambda(\mathbf{H}_2)$, as given in (3.7).

3.2– Ordered Successive Interference Cancellation

3.2.1 – The Geometry of Optimal Ordering

As mentioned in Chapter 1, D-BLAST was the first scheme to be proposed by Foschini. Given its detection complexity, V-BLAST ended up being the standard architecture for SM. The detection algorithm first proposed in [120], [85], uses the principles of SIC, already known in ISI control and MUD and is known as the V-BLAST detector (as mentioned, in this thesis the name V-BLAST is identified with that particular detection method). The general principle of SIC is that an initial "best" layer is detected and then, assuming that the symbol was correctly detected, the interference caused by that symbol is replicated and subtracted from all the other layers. The procedure is then applied to the "next best" layer: one symbol more is detected, its interference recreated and then subtracted from the remaining ones.

One important question that arises is the one of determining the order of detection of the N_R antennas. For a MIMO $n \times n$ system one has to find the optimum

permutation $\Pi(k)$ of the column indexes $\{1,2,\cdots,n\}$ that minimises the SER amid all the $n!$ possible permutations. An exhaustive search over all the permutations would rapidly become unbearable as n increases. The optimal solution to this problem was found early on in [120], [85], in the first implementations of the V-BLAST detector.

The optimal criterion at each stage is to select the layer that less emphasises the noise power after a ZF or a MMSE filter. Consider the following example with input data $\mathbf{x} = [1 \quad 1 \quad 1]^T$ and a noise vector that does not induce an error in the MLD sense, i.e., that does not take the point out of its Voronoi region:

$$\mathbf{y} = \begin{bmatrix} -0.3 \\ 2.4 \\ -1.28 \end{bmatrix} = \underbrace{\begin{bmatrix} -0.97 & 0.48 & 0.31 \\ 1.35 & 0.12 & 1.43 \\ -1.04 & 1.2 & -1.94 \end{bmatrix}}_{\mathbf{H}} \begin{bmatrix} x_1 \\ x_2 \\ x_2 \end{bmatrix} + \underbrace{\begin{bmatrix} 0.5 \\ -0.5 \\ 0.5 \end{bmatrix}}_{\mathbf{n}}. \tag{3.30}$$

Considering that ZF is used,

$$\mathbf{W}_{ZF}^{(1)} = \mathbf{H}^{+} = \begin{bmatrix} -1.0296 & 0.2954 & 0.3823 \\ 0.5980 & 0.8239 & 0.5118 \\ 0.9219 & 0.3512 & -0.4039 \end{bmatrix} \begin{array}{l} \leftarrow \left\|\mathbf{w}_1(1,:)\right\|^2 = 1.2936 \\ \leftarrow \left\|\mathbf{w}_1(2,:)\right\|^2 = 1.2983 \\ \leftarrow \left\|\mathbf{w}_1(3,:)\right\|^2 = 1.1363 \end{array},$$

where the energy of each row in the filtering matrix is indicated on the right.

The lowest noise enhancement factor is the one associated with the third row (i.e., the third layer), so this third symbol is decided via a decision threshold to the alphabet as[21] $\hat{\mathbf{x}}(3) = Q_{\mathcal{A}}[W_{ZF}^{(1)}\mathbf{y}] = 1$. Next, the effect of that symbol, after, is subtracted from the other layers:

$$\mathbf{y}^{(2)} = \mathbf{y} - \mathbf{H}(:,3)\,\hat{\mathbf{x}}(3) = \mathbf{y} - \begin{bmatrix} 0.31 \\ 1.43 \\ -1.94 \end{bmatrix} 1 = \begin{bmatrix} 0.01 \\ 0.97 \\ 0.66 \end{bmatrix}.$$

The third generator vector in the channel matrix is now nulled:

$$\mathbf{H}^{(2)} = \begin{bmatrix} -0.97 & 0.48 & 0 \\ 1.35 & 0.12 & 0 \\ -1.04 & 1.2 & 0 \end{bmatrix},$$

[21] The notation is slightly abused, as the quantisation is made on the third element of $W_{ZF}^{(1)}\mathbf{y}$.

and the associated ZF matrix is now

$$\mathbf{W}_{ZF}^{(2)} = \begin{bmatrix} -0.2185 & 0.6045 & 0.0270 \\ 0.0837 & 0.6279 & 0.7371 \\ 0 & 0 & 0 \end{bmatrix} \begin{matrix} \leftarrow \left\|\mathbf{w}_2(1,:)\right\|^2 = 0.4139 \\ \leftarrow \left\|\mathbf{w}_2(2,:)\right\|^2 = 0.9446 . \end{matrix}$$

At this stage one observes that the first row is the one that less enhances the noise and thus $\mathbf{x}(1)$ (element transmitted in the first layer) is now decided as $\hat{\mathbf{x}}(1) = Q[W_{ZF}^{(2)}\mathbf{y}^{(2)}] = 1$ and its interference subtracted from $\mathbf{y}^{(2)}$:

$$\mathbf{y}^{(3)} = \mathbf{y}^{(2)} - \mathbf{H}(:,1)\,\hat{\mathbf{x}}(1) = \begin{bmatrix} 0.01 \\ 0.97 \\ 0.66 \end{bmatrix} - \begin{bmatrix} -0.97 \\ 1.35 \\ -1.04 \end{bmatrix} 1 = \begin{bmatrix} 0.98 \\ -0.38 \\ 1.70 \end{bmatrix}.$$

Now, the first generator of $\mathbf{H}$ is zeroed

$$\mathbf{H}^{(3)} = \begin{bmatrix} 0 & 048 & 0 \\ 0 & 0.12 & 0 \\ 0 & 1.2 & 0 \end{bmatrix},$$

and the corresponding pseudo-inverse is

$$\mathbf{W}_{ZF}^{(3)} = \begin{bmatrix} 0 & 0 & 0 \\ 0.2849 & 0.0712 & 0.7123 \\ 0 & 0 & 0 \end{bmatrix} \leftarrow \left\|\mathbf{w}_2(2,:)\right\|^2 = 0.5936 .$$

Finally, $\hat{\mathbf{x}}(2) = Q[W_{ZF}^{(3)}\mathbf{y}^{(3)}] = 1$, that is once again a correctly detected symbol.

The ordering strategy described in this example makes use of algebraic arguments and is a direct application of what until [120] was a rule of thumb in MUD, but whose optimality had not been proven. The rule consists of selecting at each step the vector that minimises noise enhancement and in [120] the authors pointed out that the SNR at layer i is

$$\rho_{i,\mathrm{OSIC}} = \frac{E[x_i^2]}{\sigma_n^2 \sum_{l=1}^{N_T} w_i^2} = \frac{E[x_i^2]}{\sigma_n^2 \left\|\mathbf{w}_i\right\|^2}, \tag{3.31}$$

and use (3.31) to justify the optimality of the criterion.

In the following it is shown that further insight concerning this optimisation process can be enlightened, and indeed proven to be optimal, if a geometric perspective is applied using the projection tools introduced in section 3.1.5 and using the geometric ideas of the Babai's nearest plane algorithm [169], [113] (ch.2) in algorithmic number theory, which corresponds to SIC in MIMO, as first noticed by [106], [121].

In order to minimise the error probability when deciding layer j, the generator vector $\mathbf{h}_j$ to be selected at any given decision step k, with $k \in \{1,2,\cdots,n\}$, should be the vector that maximises the projection onto the orthogonal space to the space spanned by the matrix that remains after that same vector is taken out from $\mathbf{H}$.

The initial step is to find the column vector $\mathbf{h}_1$ that, when removed from $\mathbf{H}$, transforms $\mathbf{H}$ into $\mathbf{H}_{\bar{1}}$ (as $\mathbf{H}_{\bar{j}}$ denotes the matrix that is obtained from $\mathbf{H}$ after removing column j). $\mathbf{H}_{\bar{1}}$ is the generator of an $(n-1)$-dimensional lattice Λ_{n-1}. Hence, the original lattice can be written in the form

$$\Lambda = \Lambda_{n-1} + i\mathbf{h}_1, i \in \mathbb{Z}, \tag{3.32}$$

signifying that Λ can be created from the *union* of translates of the Λ_{n-1} sublattice.

Once a decision is produced for one layer, the subsequent step is to repeat the process, now in the sublattice with basis $\mathbf{H}_{\bar{j}}$, i.e., by removing generator $\mathbf{h}_j$ from the set. The process repeats itself until a decision is made in a one-dimensional lattice, corresponding to the decision of the last layer to be detected.

Figure 3.7 depicts SIC applied to a lattice partitioned as in (3.32). In a first stage the nearest hyperplane is found and a decision for the layer associated to $\mathbf{h}_j$ is produced. In a second stage, depicted at the bottom of Figure 3.7, the same procedure is applied but now conducted in the sublattice Λ_{n-1}.

Figure 3.8 shows the SIC decision region for the origin of the lattice with basis

$$\mathbf{H} = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}. \tag{3.33}$$

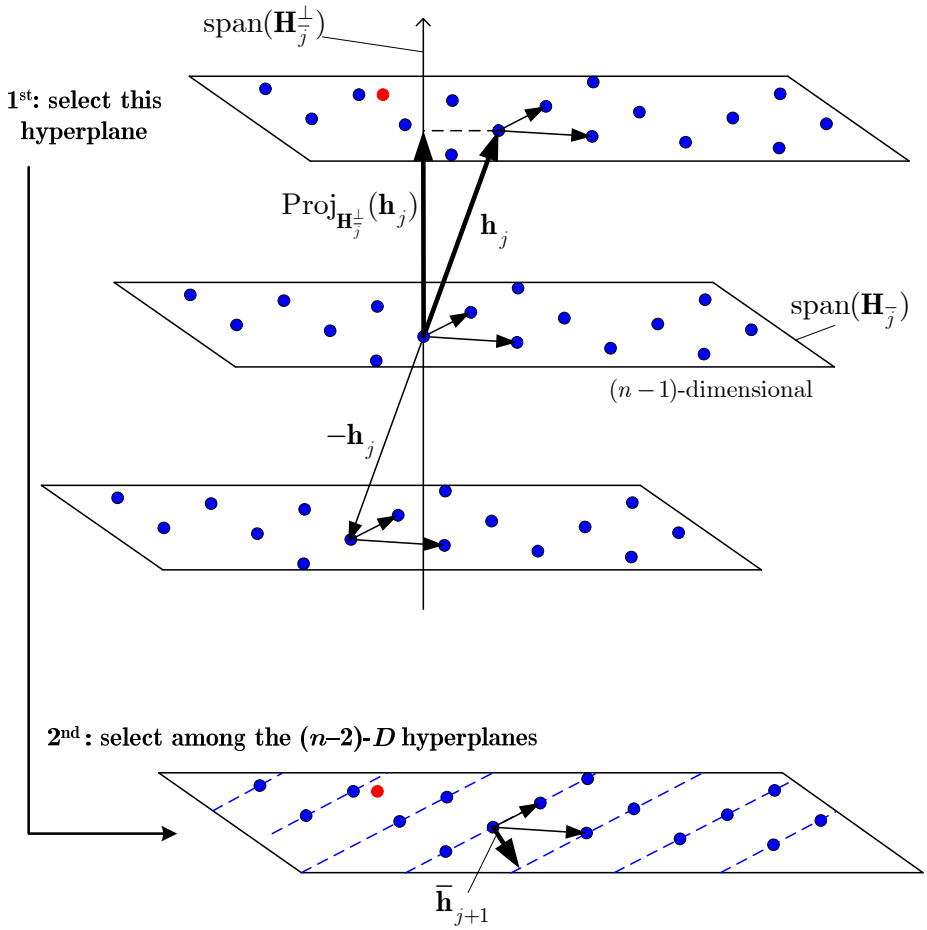


Figure 3.7: The nearest plane algorithm with sorting. Choosing the j^{th} generator vector that maximises the distance between parallel hyperplanes. The lattice is the union of such translates.

The example shows a target point located in a region where SIC outputs an erroneous decision. The first SIC step in the example in Figure 3.8 is to select which plane is the nearest one to the target point. In the example, SIC would decide for plane 1 while the Voronoi region indicates that the correct point lies in plane 2.

The diversity attained by SIC is $N_R - N_T + 1$ and sorting the layers does not contribute to any improvement in this respect, as recently proven in [84]. Sorting can only yield a power gain in SM detection.

The decision regions associated to SIC are hyper-rectangular and it is not difficult to perceive (e.g., from figures 3.7 and 3.8) that these decision regions are unequivocally defined by the Gram-Schmidt vectors of the basis of the lattice (e.g.,[160]).

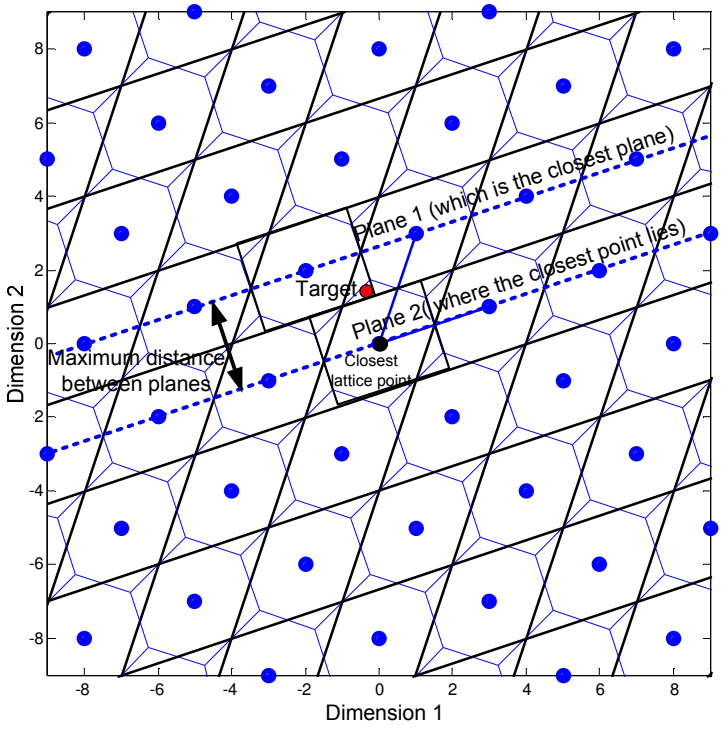


Figure 3.8: Errors events in SIC. Plane 1 is selected because it is the closest plane, however, the closest lattice point lies in plane 2. The SIC decision region for the origin is shown.

The fastest implementation of the original OSIC idea was provided in [170] and was made cubic in n , i.e., with complexity $\mathcal{O}(n^3)$, nevertheless other $\mathcal{O}(n^3)$ algorithms were known for OSIC much before (c.f. [95] (p.39) and references therein). Ling et al. also proposed an OSIC algorithm with $\mathcal{O}(n^3)$ complexity based on the geometric insights offered by the dual lattice [145], [171]. In doing that, the same optimal ordering known for OSIC [85] is proven and the same performance is attained without needing a matrix inversion for each layer to be detected. This approach makes use of the shortest vector in the dual basis at each detection step.

One can now formalise SIC in a very concise manner; the k^{th} index for the permutation is then selected from

$$\Pi(k) = \underset{j \in \mathcal{A}_k}{\arg\max} \left\{ \left\langle \mathbf{h}_j^T, \text{Proj}_{\mathbf{H}_{\bar{j}}^{\perp}}(\mathbf{h}_j) \right\rangle \right\}. \tag{3.34}$$

where $\mathcal{A}_k$ is the set of columns that have not been chosen yet. From section 3.1.5, (3.34) becomes

$$\Pi(k) = \underset{j \in \mathcal{A}_k}{\arg\max} \left\{ h_j^T \left(\mathbf{I} - \mathbf{H}_{k,j}^T (\mathbf{H}_{k,j}^T \mathbf{H}_{k,j})^{-1} \mathbf{H}_{k,j}^T \right) h_j \right\}, \tag{3.35}$$

which is a very concise expression that summarises the entire OSIC with optimal ordering [172]. Starting with $A_1 = \{1, 2, \cdots, n\}$ (i.e., with all the columns of $\mathbf{H}$), the set A_k is reduced by one element each time a column is selected, and continues until only one is left. Although concise, this formulation for finding the permutation $\Pi(k)$ does not lead to a practical implementation.

There is however a very elegant way of finding $\Pi(k)$ remembering that the distance between hyperplanes in the primal lattice is established by the lattice points in the dual (as proved in Chapter 2). Selecting the smallest basis vector in the dual basis ensures that the decision for that layer will be made from selecting between the most distant hyperplanes associated to that basis. Nonetheless, it is important to highlight that these are *not* necessarily the most distant hyperplanes in the lattice. This observation confirms why there is room for improving a receiver based on the OSIC principle.

It is thus natural to look for short vectors in the dual lattice other than the generators constituting the basis. Shorter vectors in the dual lattice would maximise the distance between the parallel hyperplanes and thus minimise erroneous decisions. Finding shorter vectors in the dual lattice is accomplished by means of lattice-reduction-aided (LRA) techniques, which will be presented next. Lattice reduction provides an equivalent basis with shorter (and more orthogonal) generator vectors.

It is noteworthy that the geometric interpretation presented in this section also sheds light onto the finding by Taherzadeh et al. that reducing the dual matrix is preferable to reducing the primal basis [173], [96].

3.3 – Gram-Schmidt Orthogonalisation and QR Decomposition

The Gram-Schmidt (GS) orthogonalisation (Algorithm 3.1) is a well known method that takes one set of generating vectors of space and obtains another set of vectors that span the same space but which are all mutually orthogonal. Notice that although the new basis spans the same *continuous* real (or complex) space, it does *not* span the lattice. In general, the GS vectors are not members of the lattice and therefore cannot be members of any of its bases. Finding a basis that is close to orthogonal while still spanning the same *discrete* space is the much more difficult problem of *lattice reduction*, which will be described in section 3.4.

The Gram-Schmidt vectors process can create a matrix $\mathbf{Q}$, with all columns mutually orthogonal, i.e., $\mathbf{Q}^H\mathbf{Q} = \text{diag}(\mathbf{q}_1^H\mathbf{q}_1, \cdots, \mathbf{q}_n^H\mathbf{q}_n)$. However, it is possible to make its column vectors orthonormal, i.e., $\mathbf{Q}^H\mathbf{Q} = \mathbf{I}$ and $\left\|\mathbf{q}_i\right\| = 1$. The two sets of vectors of the two versions are obviously related by the respective norms. The matrices that perform the transformation of the original matrices to the orthogonal or orthonormal forms are triangular in each of the two cases. The relation between the two triangular matrices is less obvious, though important in the MIMO context.

The orthogonal version is *i)* relevant in lattice reduction techniques such as the LLL algorithm, and *ii)* an essential tool in the interpretation of SIC. On the other hand, the orthonormal form of GS orthogonalisation corresponds to the QR decomposition and is *i)* much used in sorted or unsorted OSIC detection, and *ii)* central to sphere decoding.

Algorithm 3.1 computes the set of orthogonal vectors as

$$\overline{\mathbf{h}}_j = \mathbf{h}_j - \sum_{k=1}^{j-1} \frac{\left\langle h_j, \overline{h}_k \right\rangle}{\left\langle \overline{h}_k, \overline{h}_k \right\rangle} \overline{h}_k = \mathbf{h}_j - \sum_{k=1}^{j-1} \mu_{j,k} \overline{\mathbf{h}}_k \,. \tag{3.36}$$

In matrix form, the original column vectors can be related with the GS vectors by

$$\left[\mathbf{h}_1\ \mathbf{h}_2\ \mathbf{h}_3 \cdots \mathbf{h}_n\right] = \underbrace{\left[\bar{\mathbf{h}}_1\ \bar{\mathbf{h}}_2\ \bar{\mathbf{h}}_3 \cdots \bar{\mathbf{h}}_n\right]}_{\substack{\text{Orthogonal but} \\ \text{not orthonormal} \\ \text{columns}}} \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & & \mu_{n,2} \\ 0 & 0 & 1 & \cdots & \mu_{n,3} \\ 0 & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.37}$$

Note that $\det(\mathbf{H}) = \det(\bar{\mathbf{H}})$, as the the upper triangular (u.t.) matrix has unit determinant.

An orthonormal basis can also be constructed from the GS vectors if they are normalised:

$$\mathbf{q}_j = \frac{\bar{\mathbf{h}}_j}{\left\|\bar{\mathbf{h}}_j\right\|} \quad , \quad j = 1,2,\cdots,n\,. \tag{3.38}$$

GS orthogonalisation can also be used to compute the QR decomposition of a channel matrix as

$$\mathbf{H} = \mathbf{QR}\,, \tag{3.39}$$

with $\mathbf{Q}$ orthogonal and $\mathbf{R}$ u.t.

ALGORITHM 3.1: GRAM-SCHMIDT ORTHOGONALISATION

Input : linearly independent vectors $\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_n \in \mathbb{R}^n$

Output: Orthogonal basis $\bar{\mathbf{H}} = [\bar{\mathbf{h}}_1, \bar{\mathbf{h}}_2, \cdots, \bar{\mathbf{h}}_n] \in \mathbb{R}^n$ and coefficients $\mu_{j,k} \in \mathbb{R}$

$\bar{\mathbf{h}}_1 = \mathbf{h}_1$

for $j = 2 : n$

  $\bar{\mathbf{h}}_j = \mathbf{h}_j$

  for $k = 1 : j-1$

$$\mu_{j,k} = \frac{h_j \cdot \bar{h}_k}{\bar{h}_k \cdot \bar{h}_k}$$

$$\bar{\mathbf{h}}_j = \mathbf{h}_j - \sum_{k=1}^{n} \mu_{j,k} \cdot \bar{\mathbf{h}}_k$$

  end

end

To compute (3.39) one starts by computing the GS vectors using

$$\bar{\mathbf{h}}_j = \mathbf{h}_j - \sum_{k=1}^{N} \left\langle \mathbf{h}_j, \mathbf{q}_k \right\rangle \quad , \quad j = 1,2,\cdots,n\,. \tag{3.40}$$

Moreover, each of the n vectors of the original basis $\mathbf{H}$ can be expressed in terms of the orthonormal vectors $\mathbf{q}_j$ as

$$\mathbf{h}_j = \left\langle \mathbf{h}_j, \mathbf{q}_1 \right\rangle \mathbf{q}_1 + \ \cdots \ + \left\langle \mathbf{h}_j, \mathbf{q}_{j-1} \right\rangle \mathbf{q}_{j-1} + \left\| \bar{\mathbf{h}}_j \right\| \mathbf{q}_j\,. \tag{3.41}$$

This relation can be conveniently written in matrix form as

$$\left[\mathbf{h}_1\ \mathbf{h}_2\ \mathbf{h}_3 \cdots \mathbf{h}_n\right] = \underbrace{\left[\mathbf{q}_1\ \mathbf{q}_2\ \mathbf{q}_3 \cdots \mathbf{q}_n\right]}_{\substack{\mathbf{Q} \text{ with} \\ \text{orthonormal columns}}} \begin{bmatrix} \left\|\bar{\mathbf{h}}_1\right\| & \left\langle \mathbf{h}_2, \mathbf{q}_1 \right\rangle & \left\langle \mathbf{h}_3, \mathbf{q}_1 \right\rangle & & \left\langle \mathbf{h}_n, \mathbf{q}_1 \right\rangle \\ 0 & \left\|\bar{\mathbf{h}}_2\right\| & \left\langle \mathbf{h}_3, \mathbf{q}_2 \right\rangle & & \left\langle \mathbf{h}_n, \mathbf{q}_2 \right\rangle \\ 0 & 0 & \left\|\bar{\mathbf{h}}_3\right\| & \cdots & \left\langle \mathbf{h}_n, \mathbf{q}_3 \right\rangle \\ 0 & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \left\|\bar{\mathbf{h}}_n\right\| \end{bmatrix}. \tag{3.42}$$

Since $\det(\mathbf{Q}) = 1$, the volume of the lattice is the product of the orthogonal vectors

$$\mathrm{vol}(\Lambda) = \prod_{i=1}^{n} \left\|\hat{\bar{\mathbf{h}}}_i\right\|, \tag{3.43}$$

which corresponds to the volume of the hyper-rectangular decision regions in SIC.

A comparison of (3.36) with (3.40) reveals that

$$\mu_{j,k}\bar{h}_k = \left\langle \mathbf{h}_j, \mathbf{q}_k \right\rangle = \mathrm{Proj}_{\mathbf{q}_k}(\mathbf{h}_j)\,, \tag{3.44}$$

each of which is the projection of the original generator vector onto the one-dimensional space spanned either by $\mathbf{q}_k$ or $\mathbf{h}_k$.

3.4 – Lattice-Reduction-Aided Detection

As was exemplified in Figure 3.3, the two bases given by (3.7) generate the same lattice but their fundamental regions have different coverage. In order to maximise the coverage of the MLD region, one is interested in bases with vectors that are both short and close to orthogonal, which is called a *reduced basis.* Figure 3.9 shows a lattice with a rather "skewed" basis and a reduced basis.

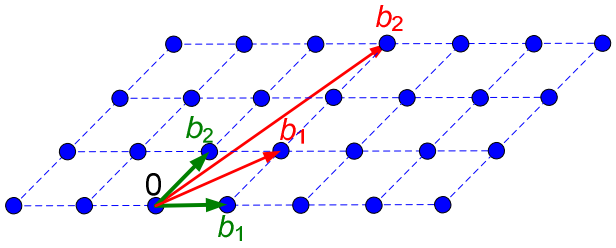


Figure 3.9: A reduced basis (green) and a skewed basis (red) for the same lattice.

It was seen in Chapter 2 that two different bases of a lattice are related by a unimodular transformation $\mathbf{M}$. In particular, the two basis in (3.7) are related by

$$\mathbf{H}_1 = \mathbf{H}_2\mathbf{M} \Leftrightarrow \begin{bmatrix} 6 & 2 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 6 & 8 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \tag{3.45}$$

and in this case it is easy to see that $\det(\mathbf{M}) = 1$.

As observed in section 3.1.2, it is preferable to invert a well-conditioned channel matrix, and therefore having a more orthogonal basis contributes to a smaller noise enhancement factor whenever a ZF or a MMSE filter are applied (standalone or included in the OSIC stages). In LRA receivers a pre-processing stage is introduced before the detection algorithm, as shown in Figure 3.10.

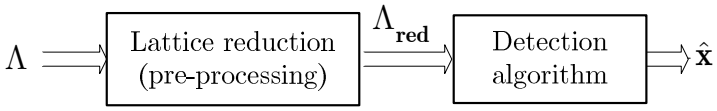


Figure 3.10: MIMO detection with lattice-reduction pre-processing.

The application of lattice-reduction-aided (LRA) techniques to MIMO detection was pioneered by Yao and Wornell in 2002 [126],[174] and since then the research in LR applications to MIMO has boomed not only for the detection but also for precoding in the BC (as mentioned in Chapter 1). These authors applied the Lenstra Lenstra Lovász reduction (LLL, also sometimes denoted as L^3) [129] to reduce the channel matrix. In 2007, Seysen's reduction was simultaneously re-discovered for MIMO in [127] and in [128]. This technique is based on the simultaneous reduction of both the primal and

dual basis. One other important lattice reduction approach (LR) that delivers a more reduced basis than the others is the Korkin-Zolotarev reduction (e.g., [135] (ch. 3)), however it is not used in communication applications because of its higher complexity. The quality of the output of a LR algorithm can be measured by the *orthogonality defect*, defined as [113] (p. 131)

$$OD(\mathbf{H}) = \frac{\prod_{i=1}^{n} \left\| \mathbf{h}_i \right\|}{\det(\mathbf{H})}. \tag{3.46}$$

Shorter generator vectors correspond to a lower orthogonality defect. Clearly, $OD(\mathbf{H}) \geq 1$, with equality attained only by the $\mathbb{Z}^n$ lattice.

An overview of the applications of lattice reduction techniques in MIMO (including SM and BC) exists in [175]. LRA detection achieves the maximum diversity available in SM, as proved by Taherzadeh et al. [173][22] for the case of LLL reduction (Seysen's algorithm and Korkin-Zolotarev also achieve that maximum diversity since, on average, they output bases even closer to orthogonal bases).

The idea is that the system model can be re-written as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \Leftrightarrow \underbrace{\mathbf{H}\mathbf{M}}_{\mathbf{H}_{\text{red}}} \underbrace{\mathbf{M}^{-1}\mathbf{x}}_{\mathbf{z}} + \mathbf{n} \Leftrightarrow \mathbf{H}_{\text{red}}\mathbf{z} + \mathbf{n} \tag{3.47}$$

In this model, $\mathbf{z}$ is a modified data vector that can be detected with a lower SER than would $\mathbf{x}$ without LR. This is true regardless the type of receiver that follows the LR pre-processing (usually ZF, MMSE or OSIC). The original data vector can then be recovered from $\mathbf{z}$ noting that

$$\mathbf{z} = \mathbf{M}^{-1}\mathbf{x} \quad \Rightarrow \quad \mathbf{x} = \mathbf{M}\mathbf{z} \tag{3.48}$$

Because M-QAM constellations and their PAM equivalent alphabets are defined without the origin and have non unitary distance between the symbols (c.f. section

[22] The same result was also proved by Ma and Zhang in [244] for the Complex-LLL algorithm (CLLL), where the real equivalent model is not used and LLL is applied directly to the complex lattice.

2.2.1), in order to apply the lattice tools as in (3.47)-(3.48), it is necessary to make a translation of the constellation, creating the modified received vector

$$\mathbf{y}_{\mathbf{red}} = \frac{1}{2}\big(\mathbf{y} + \mathbf{H}\cdot\mathbf{1}\big) = \frac{1}{2}\big(\mathbf{Hx} + \mathbf{n} + \mathbf{H}\cdot\mathbf{1}\big), \tag{3.49}$$

where $\mathbf{1}$ is the column vector of n elements all equal to 1.

Now, in the case of a ZF criterion,

$$\mathbf{z} = \mathbf{H}^{+}_{\mathbf{red}}\mathbf{y}_{\mathrm{red}}\,, \tag{3.50}$$

and in performing

$$\hat{\mathbf{x}} = 2\mathbf{M}\underbrace{Q_{\mathbb{Z}}(\mathbf{z})}_{\hat{\mathbf{z}}} - \mathbf{1}\,, \tag{3.51}$$

the symbol $\hat{\mathbf{z}}$ is detected and put back in the alphabet $\mathcal{A}$.

The LLL algorithm was first derived for integer lattices and then applied to real lattices. It has also been shown that a complex LLL algorithm can be defined and that by applying it directly to $\mathbf{H}_c$, the complexity becomes half of the one involved in the application of Algorithm 3.2 to the real equivalent lattice [176].

The LLL algorithm can be seen as an extension to higher dimensions of Gauss's algorithm [113] (p. 28), which operates in two dimensions only (c.f. example in Figure 3.11). It is also noteworthy that the LLL algorithm can be derived by making appropriate changes to the GS orthogonalisation (Algorithm 3.1), as recently shown by Fischer [177] and is also closely related to sorting in OSIC [178].

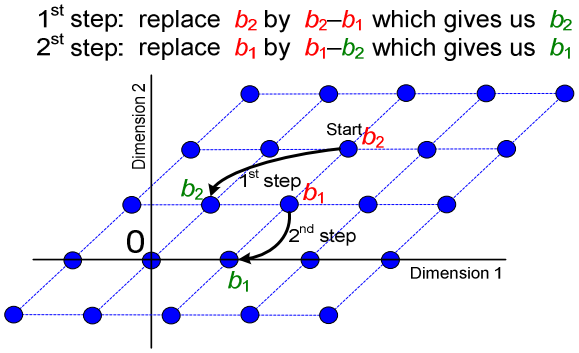


Figure 3.11: The Gauss' algorithm (i.e., LLL in 2D).

Ling et al. recently proved that the complexity of the LLL reduction is $\mathcal{O}(n^4 \log n)$ not only for integer lattices (e.g., [179]) but also proved that for Gaussian lattices [180]. They further proposed a change to the algorithm that maintains a similar performance while having complexity $\mathcal{O}(n^3 \log n)$. It was shown in [181] that for some instances of lattices, the complexity of the LLL algorithm for non-integer matrices is not polynomial but that probability tends to zero.

ALGORITHM 3.2: LENSTRA LENSTRA LOVÁSZ (LLL)

Input : a basis $\mathbf{H}$ with generator vectors $\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_n \in \mathbb{R}^n$ in its columns

Output: a ζ-LLL reduced basis $\mathbf{H}_{\text{red}}$, a unimodular matrix $\mathbf{M}$

1: (Preliminaries)

Compute the GS orthogonal vectors $\overline{\mathbf{h}}_1, \overline{\mathbf{h}}_2, \cdots, \overline{\mathbf{h}}_n$ using Algorithm 3.1

Set $\mathbf{M} = \mathbf{I}_n$

2: (Reduction step)

for $i = 2$ to n

for $j = i-1$ down to 1

$$\mathbf{h}_i = \mathbf{h}_i - \left\lceil \frac{\left\langle \mathbf{h}_i, \overline{\mathbf{h}}_j \right\rangle}{\left\langle \overline{\mathbf{h}}_j, \overline{\mathbf{h}}_j \right\rangle} \right\rfloor \mathbf{h}_j$$

$$\mathbf{m}_i = \mathbf{m}_i - \left\lceil \frac{\left\langle \mathbf{h}_i, \overline{\mathbf{h}}_j \right\rangle}{\left\langle \overline{\mathbf{h}}_j, \overline{\mathbf{h}}_j \right\rangle} \right\rfloor \mathbf{m}_j$$

end

recompute the GS orthogonal vectors $\overline{\mathbf{h}}_1, \overline{\mathbf{h}}_2, \cdots, \overline{\mathbf{h}}_n$ using Algorithm 3.1

3: (Swap step)

if there is i such that $\zeta \left\| \overline{\mathbf{h}}_i \right\|^2 > \left\| \overline{\mathbf{h}}_{i+1} + \mu_{i+1,i} \overline{\mathbf{h}}_i \right\|^2$ then

swap columns $\mathbf{h}_i$ and $\mathbf{h}_{i+1}$

swap columns $\mathbf{m}_i$ and $\mathbf{m}_{i+1}$

go to 1

end

4: return $\mathbf{h}_1, \mathbf{h}_2, \cdots \mathbf{h}_n$ and $\mathbf{M}$

3.5– Sphere Decoding

Sphere decoding (SD) is an exact detection method (i.e., it achieves the same performance as MLD) with a complexity that, on average, is much lower than MLD. The idea is that a rigid rotation $\mathbf{Q}$ can be applied to the ensemble $\{\Lambda, \mathbf{y}\}$, for which the CVP needs to be solved, so that the lattice can be described by an equivalent lattice in u.t form. The u.t. property allows describing the norm of any lattice point to be detected as a sum that can be computed incrementally, taking in consideration the cumulative effect of each vector components. Consider now that an upper bound (UB) on the norms is established. The u.t. property of the basis allows all the possible values in the last component of the data vector, $x(n)$, to be detected. As the norm can be computed as a sum of "ordered" contributions, if some of the tested values in $x(n)$ generates a total vector norm that is larger than the UB, then those values of $x(n)$ need not to be considered further as possible values in the solution. This procedure can extended to the next layer $x(n-1)$, where only the possible values of $x(n)$ are considered. In conclusion, finding vectors with norm smaller then the UB is a problem that can be solved by expanding and pruning a tree that represents the lattice points. All these ideas can be converted to the CVP, if the lattice is shifted to the target $\mathbf{y}$.

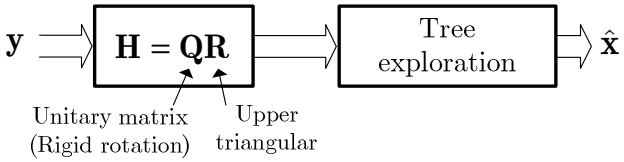


Figure 3.12: Receiver based on sphere decoding.

A sphere decoder has the structure shown in Figure 3.12. After traversing the tree with a particular symbol enumeration, the MLD solution is always found if the initial radius that is chosen is large enough to contain a lattice point inside the hypersphere. Figure 3.13 gives an example tree associated with 3×3 antenna and 4-PAM, showing the branches that have been expanded at each tree level.

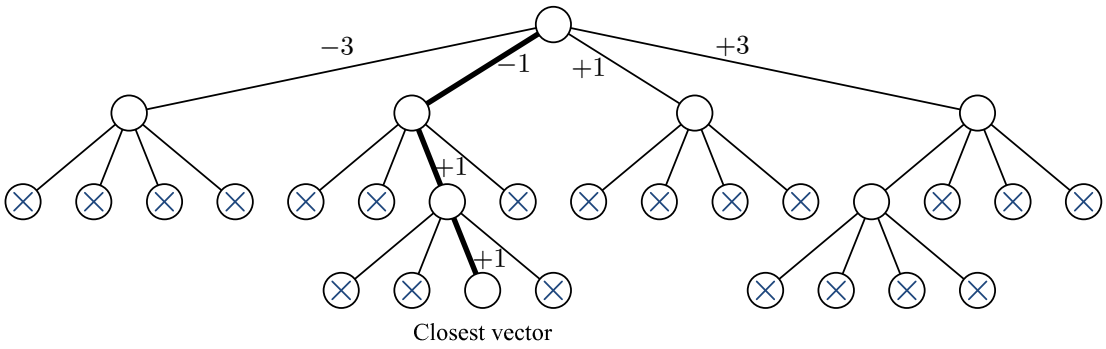


Figure 3.13: Tree exploration of a tree with 3 layers, considering a 4-PAM alphabet.

As mentioned previously, one can define an UB for the radius (or, equivalently, for the squared radius) of the sphere around the received point, i.e.,

$$\left\|\mathbf{y}-\mathbf{H}\mathbf{x}\right\|^2 \leq \xi^2 \tag{3.52}$$

$$\left\| \mathbf{y} - [\mathbf{Q}_1 \ \mathbf{Q}_2] \begin{bmatrix} \mathbf{R} \\ 0 \end{bmatrix} \mathbf{x} \right\|^2 \leq \xi^2 \,. \tag{3.53}$$

Applying the inverse rotation $\mathbf{Q}^H$ (remembering that $\mathbf{Q}$ is unitary, or orthogonal in the real case),

$$\begin{aligned} &\left\| \begin{bmatrix} \mathbf{Q}_1^H \\ \mathbf{Q}_2^H \end{bmatrix} \mathbf{y} - \begin{bmatrix} \mathbf{R} \\ 0 \end{bmatrix} \mathbf{x} \right\|^2 \leq \xi^2 \\ \Leftrightarrow &\left\| Q_1^H \mathbf{y} - \mathbf{R}\mathbf{x} \right\|^2 + \left\| \mathbf{Q}_2^H \mathbf{y} \right\|^2 \leq \xi^2 \end{aligned} \tag{3.54}$$

If one defines $\mathbf{y}' = Q_1^H \mathbf{y}$ and $\xi'^2 = \xi^2 - \left\|\mathbf{Q}_2^H \mathbf{y}\right\|^2$, then the CVP can be written as

$$\left\|\mathbf{y}'-\mathbf{R}\mathbf{x}\right\|^2 \leq \xi'^2 \,. \tag{3.55}$$

Finally, remembering that $\mathbf{R}$ is u.t., the problem can be written as the sum

$$\sum_{i=1}^{m} \left(y_i' - \sum_{j=i}^{m} r_{ij} x(j) \right)^2 \leq \xi'^2 \,. \tag{3.56}$$

The complexity of sphere decoding is usually measured by the number of nodes that need to be visited in the tree until the MLD solution is found. The fact that the complexity is a random variable is a limitation of SD. To circumvent this problem, it is

possible to expand only say, K branches at each level of the tree, as is the case in the K-*best receivers* and its variations [182], [183], [184]. Nonetheless there are different approaches as to how the tree should be traversed. Historically, the Fincke-Pohst method [185] was the first to be used, followed by the more efficient Schnorr-Euchner node enumeration [106], which attains the same performance, while expanding a smaller number of tree branches. Su showed in [186], [185], that a dramatically more efficient exploration of the tree could be made if not only the channel is taken in to consideration when enumerating the symbols in the alphabet, but also the particular target point was also taken into account during that sorting process. Furthermore, Su's ordered traversal of the tree also eliminated the need for an initial radius and provides automatic *boundary control* for spherical lattice codes [81]. Recently, simplifications to the Fincke-Pohst and Schnorr-Euchner's enumerations have been proposed, eliminating about 75% of the operations previously required [187].

The average complexity of SD is exponential [188], given by $\mathcal{O}(M^{\alpha N_T})$ with $0 \leq \alpha \leq 1$ [189], however, for low dimensional lattices, that number is affordable. A celebrated improvement to SD was the development of fixed complexity sphere decoding (FCSD) by Barbero and Thompson [190]. FCSD splits the tree exploration in to two: one where all valid branches are further expanded, and a second phase, conducted for the remaining layers, where only one branch is expanded from any node. Recently, an automatic adjustment of the switching point was proposed in [191]. The performance of FCSD was described analytically in [192].

The SD principle will be applied in the next section as part of a pre-processing stage of a new receiver not to solve CVP but instead to find a set of short vectors around the origin. SD is also used in this dissertation to obtain the MLD performance curves for the more challenging configurations such as 4×4 with 64-QAM, however its complexity is not a concern in this work. For these reasons, the SD that was chosen is a simple implementation of Fincke-Pohst enumeration, such as the one given in [188],[38] (ch15) where the output of the algorithm is not just one point but the set of all points inside the defined sphere. The implementation of this SD is given in Algorithm 3.3.

ALGORITHM 3.3: SPHERE DECODING (FINCKE-POHST)

Input : $\mathbf{Q}$, orthogonal, $\mathbf{R}$, upper triangular, a target vector $\mathbf{y} = \mathbf{Q}_1\mathbf{x}$, radius ξ

Output: a MLD solution to the CVP, $\hat{\mathbf{x}}_{SD}$

1: Set $k = n$, $\xi_m'^2 = \xi^2 - \left\|Q_2\mathbf{x}\right\|^2 \frac{1}{2}, \mathbf{y}_{m|m+1} = \mathbf{y}_m$

2: (Bounds for s_k) Set $\mathrm{UB}(x_k) = \left\lfloor \frac{\xi_k' + y_{k|k+1}'}{r_{kk}} \right\rfloor, x_k = \left\lceil \frac{-\xi_k' + y_{k|k+1}'}{r_{kk}} \right\rceil - 1$

3: (Increase x_k) $x_k = x_k + 1$,

4: (Increase k) $k = k+1$

if $k = m+1$

Terminate (no lattice point found)

else go to 3

5: (Decrease k)

if $k = 1$

go to 6

else

$k = k - 1$

$y_{k|k+1}' = y_k' - \sum_{j=k+1}^{m} r_{kj} x_j$

$\xi_k'^2 = \xi_{k+1}'^2 - (y_{k+1|k+2} - r_{k+1,k+1}x_{k+1})^2$

go to 2

6: (Solution found)

return $\hat{\mathbf{x}}_{SD} = \mathbf{x}$

go to 3

The algorithm starts by detection the last element in $\mathbf{x}$. Note that the subscript in $y_{k|k+1}'$ denotes the symbol y_k', in the k^{th} layer, incorporating the effect of the layers already detected, in agreement with (3.56). In this algorithm the option was made to denote the elements in a vector by x_n instead of $x(n)$, in order to accommodate notation such as $y_{k|k+1}'$ that also reflects the updates of a vector over time or the updates of the radius over time.

3.6– Dual-Lattice-Aided Detection

The i^{th} *successive minimum* of a lattice, λ_i, has been defined at the end of section 2.1.2. Then in section 2.1.3, it was concluded that the shortest vectors in the dual lattice define families of hyperplanes in the primal lattice that maximise the density of lattice points lying on those hyperplanes. This elegant geometric relationship between the primal and the dual lattices is often overlooked in MIMO literature. This section proposes a receiver that takes advantage of this relationship in order to obtain a list of candidate solutions to the CVP. This new receiver makes simultaneous use of several hyperplanes, however, in addition to the family of hyperplanes that are furthest apart, some other families of hyperplanes associated with some of the successive minima of the dual lattice are also brought into use.

Consider the hyperplanes selected by the first L successive minima in $\Lambda^{(D)}$, i.e., $\boldsymbol{\lambda}_1$,$\cdots$ $\boldsymbol{\lambda}_L$. Finding the shortest vector in a lattice is itself a NP-hard problem, which implies the same complexity for obtaining the L shortest ones. Nevertheless, if this is only required at a pre-processing stage, and not needed for each received vector, then using a sphere decoder is acceptable. While its complexity is exponential in the dimension of the lattice, this cost is only necessary whenever the channel changes, which is appropriate for slow fading channels.

3.6.1 – Successive Minima in the Dual Lattice

The receiver consists of a pre-processing stage applying a "true" sphere decoder, not to solve the CVP, but rather to capture all the vectors of the dual lattice that are inside a hypersphere centred at the origin of the lattice (hence the reference to a "true" SD process, because it applies SD in its simplest conception, as was described in section 3.5).

Because one is interested in planes with different distances, not all the lattice points with $\left\|\mathbf{y}\right\| < \xi$ are in the set of successive minima and they need to be expunged from the

list. Because Algorithm 3.3 is being applied around the origin, it always outputs a list of (column) vectors arranged as

$$[\underbrace{\mathbf{s}_1, \mathbf{s}_2, \cdots \mathbf{s}_{N/2-1}}_{N/2-1}, \mathbf{0}, \underbrace{\mathbf{s}_{1N/2+1}, \cdots \mathbf{s}_N}_{N/2-1}], \tag{3.57}$$

where $\mathbf{0}$ denotes the origin, which is always captured in the set for any $\xi > 0$ and N is the number of lattice points inside the sphere of radius ξ. The two "sides" of the list of points output around 0 (in the form (3.57)) include the same vectors up to sign changes and therefore the selection of the first $N/2-1$ suffices. In addition to that selection, one will just take one vector for each distinctive norm, even if they correspond to linearly independent vectors. This widens the range of different distances between hyperplanes. The resulting set of vectors in the dual will be dubbed *unique successive minima* (USM). This concept is depicted in Figure 3.14, where the number of USM that are found inside the sphere is L=7.

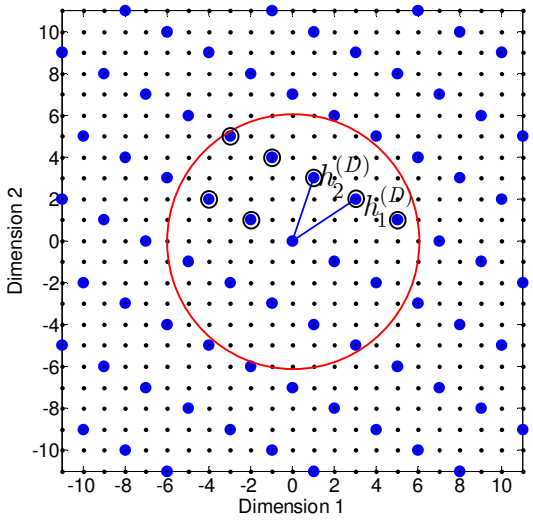


Figure 3.14: Points inside a sphere centred at the origin of the dual lattice and containing $L = 7$ USM (denoted by dots with circles around).

3.6.2– Projections Onto Hyperplanes

The L USM in the dual lattice are denoted by $\mathbf{v}_1^{(D)}, \mathbf{v}_2^{(D)}, \cdots, \mathbf{v}_L^{(D)}$. Naturally, the unit vectors which are orthogonal to the families of hyperplanes are

$$\overline{\mathbf{v}}_i^{(D)} = \mathbf{v}_i^{(D)} \Big/ \left\| \mathbf{v}_i^{(D)} \right\|. \tag{3.58}$$

Now, one further defines the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_L$, such that each one is respectively collinear with $\mathbf{v}_i^{(D)}$, but forced to have norm $d = \left\| \mathbf{v}_i^{(D)} \right\|^{-1}$, as has been suggested in Figure 2.3. Hence, from (3.58), these vectors should be

$$\mathbf{v}_i = \mathbf{v}_i^{(D)} \Big/ \left\| \mathbf{v}_i^{(D)} \right\|^2 . \tag{3.59}$$

The projections of the received vector (i.e., the target in the CVP) onto a family of $\mathcal{P}_{\mathbf{v}_i}(\nu)$ hyperplanes generates the set of projection points

$$\mathbf{y}_p(\overline{\mathbf{v}}_i, \nu) = \mathbf{y} + \left[Q_{\mathbb{Z}} \left(\frac{\left\langle \mathbf{y}, \mathbf{v}_i \right\rangle}{\left\| \mathbf{v}_i \right\|} \right) - \frac{\left\langle \mathbf{y}, \mathbf{v}_i \right\rangle}{\left\| \mathbf{v}_i \right\|} \right] \overline{\mathbf{v}}_i + \nu \, \overline{\mathbf{v}}_i , \tag{3.60}$$

where $\nu = \pm 1, \pm 2, \cdots, \pm \nu_{\max}$, and $Q_{\mathbb{Z}}(\cdot)$ denotes rounding to $\mathbb{Z}$. It is preferable to quantify the projections in terms of $\mathbf{v}_i$. Hence, the projection of the target point $\mathbf{y}$ onto the hyperplane defined by a vector $\mathbf{v}_i$ and also by the translation index ν is given by

$$\begin{aligned} \mathbf{y}_p(\mathbf{v}_i, \nu) &= \mathbf{y} + \underbrace{\left[Q_{\mathbb{Z}} \left(\frac{\left\langle \mathbf{y}, \mathbf{v}_i \right\rangle}{\left\| \mathbf{v}_i \right\|^2} \right) - \frac{\left\langle \mathbf{y}, \mathbf{v}_i \right\rangle}{\left\| \mathbf{v}_i \right\|^2} \right]}_{\Omega} \mathbf{v}_i + \nu \, \mathbf{v}_i \\ &= \mathbf{y} + \left(\Omega(\mathbf{y}, \mathbf{v}_i) + \nu \right) \mathbf{v}_i . \end{aligned} \tag{3.61}$$

Notice that, in the case of a zero noise vector, the index Ω will be *always* an integer, indicating in which hyperplane the lattice lies, for each family $\mathcal{P}_{\mathbf{v}_i}$.

3.6.3 – List of Candidate Solutions

Fixing L as the number of USM, and setting $\nu_{\max}$ as the maximum value of $|\nu|$ that will be explored, it is possible to obtain a set $\mathcal{C}$ consisting of the candidate vectors obtained from

$$\mathbf{y}_i^{(C)} = \mathbf{H} \, Q_{\mathcal{A}} \left(\mathbf{H}^{+} \mathbf{y}_p(\overline{\mathbf{v}}_i, \nu) \right) \quad , i = 1, 2, \cdots, 2L\nu_{\max}, \tag{3.62}$$

where $Q_{\mathcal{A}}()$ denotes quantization to the alphabet $\mathcal{A}$ used in each dimension. This amounts to performing zero-forcing detection not only to $\mathbf{y}$ but to the set of all projections onto $\mathcal{P}_{\mathbf{v}_i}(\nu)$. Note tha there are L families of hyperplanes being considered and that in each of them one generates $2\nu_{\max}$ projections.

This concept is depicted in Figure 3.15, which shows the projections of the target point onto the three densest families of hyperplanes with lattice points. The projections are made through the dark black segments, and for this example where $\nu = -1, 0, +1$, there are three projections along each black segment. The circle lines in Figure 3.15 correspond to the nine projections that are generated, i.e., three projections in each family of hyperplanes.

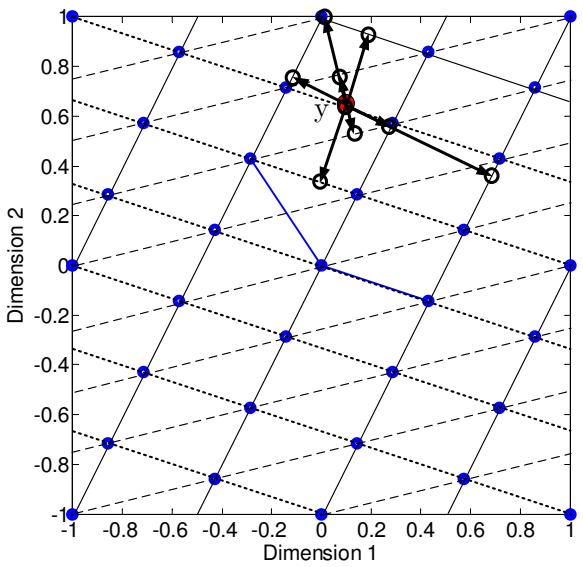


Figure 3.15: Dual-lattice-aided generation of candidate solutions considering $\nu_{\max}$=1 and considering L=3 families of hyperplanes: the two families in Figure 3.14 and also the family associated with the dual vector $h_2^{(D)} = (1,3)$.

The solution to CVP is then obtained by applying the ML principle to all the vectors in the set of candidates $\mathcal{C}$

$$\hat{\mathbf{y}} = \arg\min_{\mathbf{y}_i^{(C)} \in C} \left\{ \left\| \mathbf{y} - \mathbf{y}_i^{(C)} \right\|^2 \right\}. \tag{3.63}$$

While OSIC requires a matrix inversion when detecting each layer, the proposed receiver generates this list of candidates through a one-shot matrix product that projects the target point onto families of hyperplanes surrounding that point. Subsequently, the best candidate is selected via ZF.

The total number of candidates considered in (3.63) is given by the number of the families of hyperplanes considered (i.e., the number of USM inside a sphere) multiplied by the number parallel of hyperplanes considered (the closest one and the next ones with non-zero index ν):

$$|\,\mathcal{C}\,| = L \cdot (2\nu_{\max} + 1)\,. \tag{3.64}$$

Table 3.2 shows the number of candidates, $|\,\mathcal{C}\,|$, generated when the number of USM is set to $L = 4n$ and the maximum index of the hyperplanes in each family is $\nu_{\max} = 2$ or $\nu_{\max} = 4$.

In this dual-lattice-aided (DLA) receiver, the received vector $\mathbf{y}$ does not need to be inside the (possibly narrow) fundamental ZF decision region associated with the basis for a correct decision to occur; in fact, it suffices that at least one of the projections in the set generated by (3.61) lies inside that ZF region.

Table 3.2: Number of candidates in DLA.

	$n = 4$	$n = 6$	$n = 8$	$n = 12$
$L = 4n\,,\ \nu_{\max} = 2$	80	120	160	240
$L = 4n\,,\ \nu_{\max} = 4$	144	216	288	432

3.7 – Performance Comparison

The performance of the proposed receiver is now compared with ZF, MMSE, OSIC, LRA using LLL pre-processing with ZF and also with OSIC-ZF, and finally with MLD. Note that the MLD results are obtained by means of a SD owing to the difficulty in implementing exhaustive search for configurations with large alphabets such as 64-QAM (remembering that there are M^n possible points in the *finite* underlying lattice). Performance is assessed in terms of the (complex) symbol error rate (SER) versus the

overall SNR, ρ. Comparison are presented for 2×2, 3×3, 4×4 and 6×6 antenna systems, i.e., for real lattices with n=4, 6, 8 and 12 dimensions, in Figures 3.16 to 3.19, respectively.

It is important to note that the SER curves presented in this section, and elsewhere in this work, were obtained via Monte Carlo simulation in Matlab®. All the presented results have been obtained taking in consideration the analysis for the confidence intervals available in Jeruchim et al. [193]. These authors derived the analytical expressions for the $100 \cdot (1-\varepsilon)\%$ confidence intervals of the SER. Those expressions have also been derived and graphically represented in [194] (Annex H). For an expected $\text{SER} = 10^{-p}$, a number of symbols $N = 10^{p+2}$ was simulated. In the cases when running such a long sequence of symbols would not be feasible (i.e., for $\text{SER} \approx 10^{-5}$ with MLD), no point was plotted, unless at last an absolute number of 10 errors had been counted[23].

Additionally, the distribution functions generated in Matlab® for the Gaussian, Rayleigh and uniform random variables have been validated in [194] (Annex I) by plotting the evolution of the mean square error between the histograms generated and each one of the theoretical distribution functions.

Figures 3.16 to 3.19 allows us to observe several facts known in the literature:

- ZF, MMSE and OSIC are all shown to have the same diversity order, $d = 1$ (since $N_T = N_R$);
- The gain provided by MMSE in respect to ZF is minimal for 64-QAM in all tested configurations (in Chapter 6 it will be seen that that is not the case for QPSK and 16-QAM);
- OSIC provides a large gain in respect to both ZF and MMSE detection;
- LLL-based LRA receivers capture the same diversity as does MLD, i.e., $d = n$;
- LLL pre-processing followed by OSIC provides a large gain in comparison to using ZF after the pre-processing stage.

[23] This corresponds to a usual rule of thumb when obtaining a BER via Monte Carlo simulation, and which has been recently put to proof in [251].

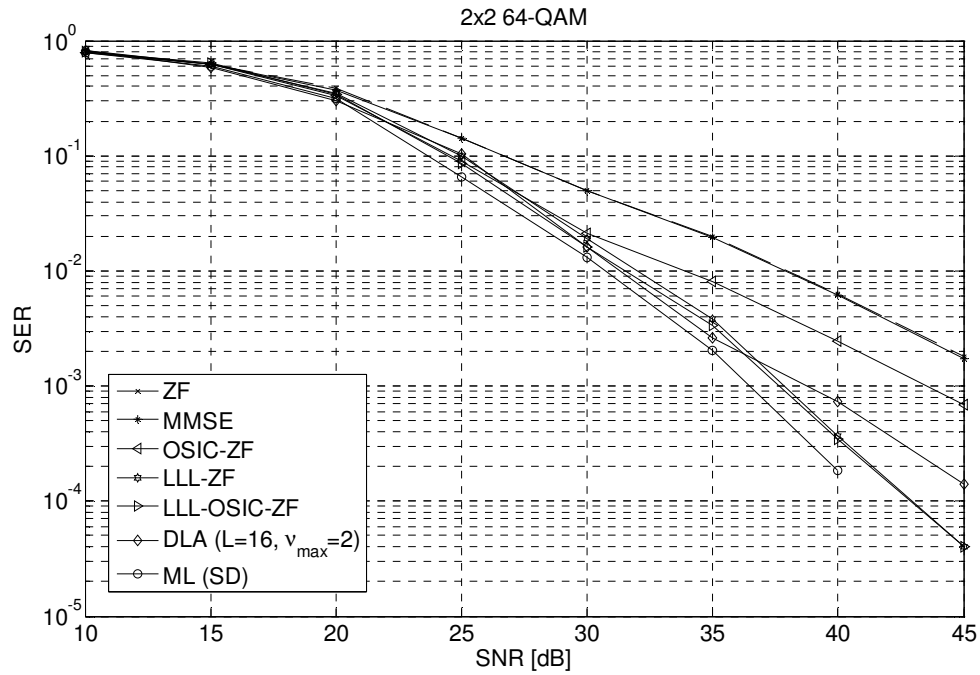


Figure 3.16: Detection in n=4 real dimensions (2×2 antennas) with 64-QAM.

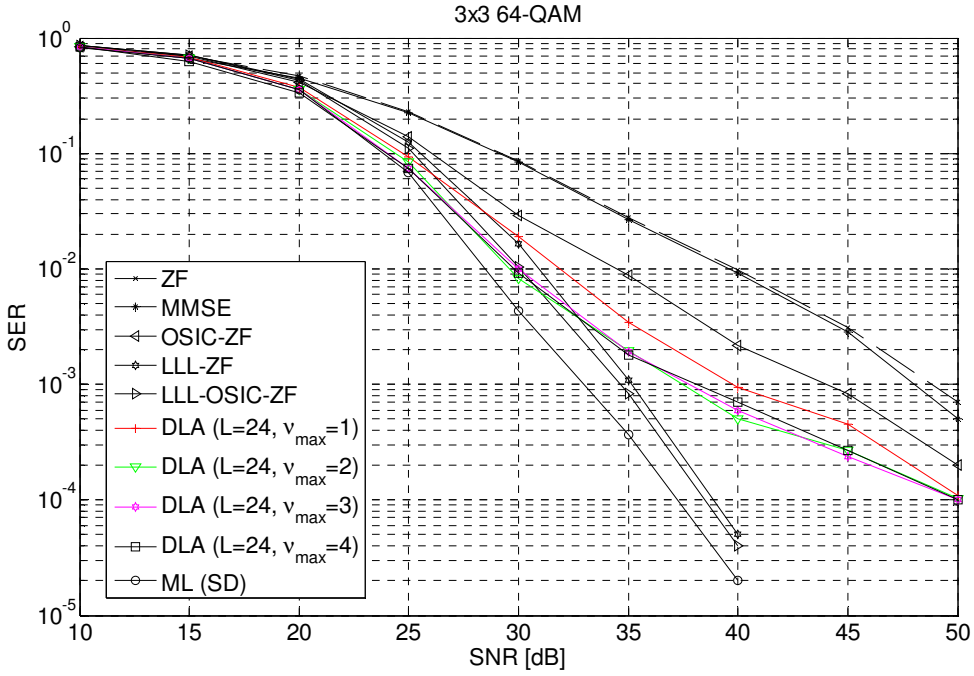


Figure 3.17: Detection in n=6 real dimensions (3×3 antennas) with 64-QAM.

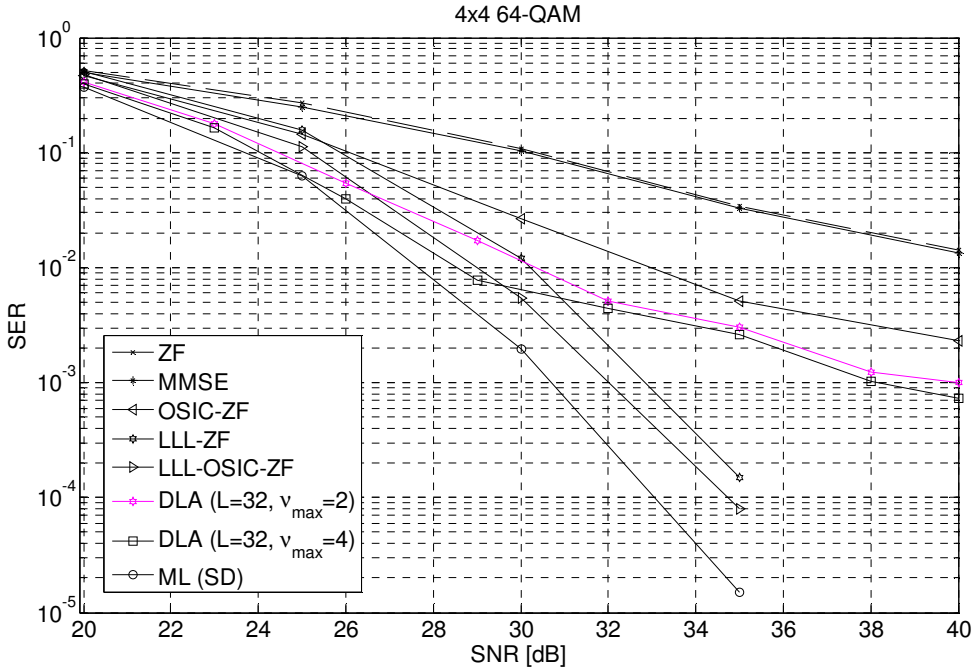


Figure 3.18: Detection in n=8 real dimensions (4×4 antennas) with 64-QAM.

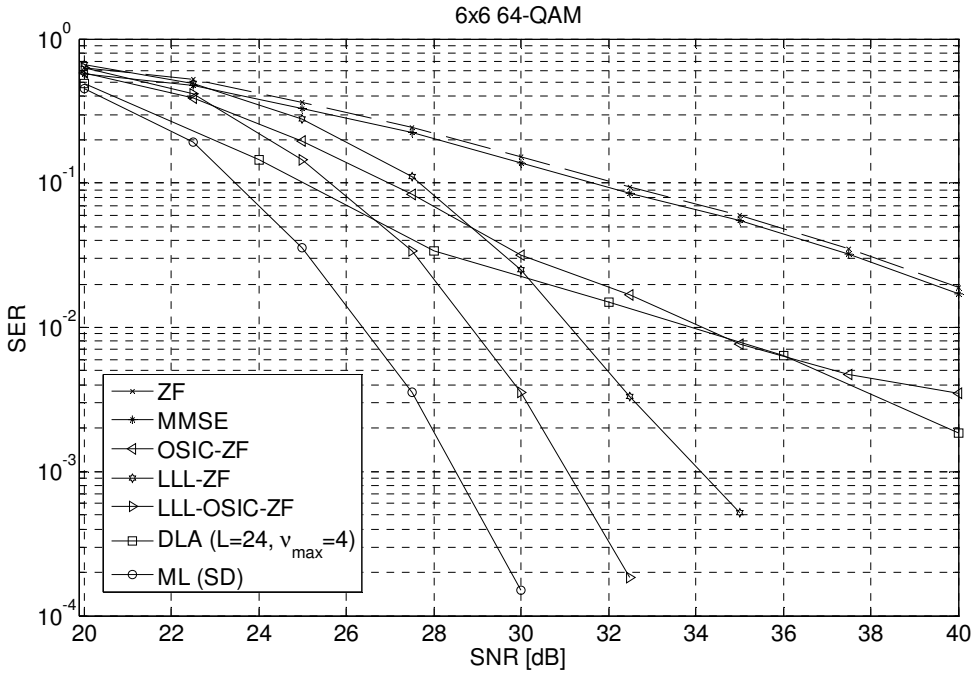


Figure 3.19: Detection in n=12 real dimensions (6×6 antennas) with 64-QAM.

The proposed DLA receiver was tested for several values of L and $\nu_{\max}$. A general rule was sought for expressing L as a (linear) function of the number of dimensions n and it was found that $L = 4n$ was the minimum scaling factor in order to offer a performance gain with respect to OSIC. One can observe that DLA detection outperforms OSIC using a reasonable number of candidates, $|C|$, obtained from the projections (3.61) and listed in Table 3.2. At $\mathrm{SER} = 10^{-3}$, the gain in respect to OSIC amounts to 5 dB with 2×2 and 3×3 antennas, and is 4dB with 4×4 antennas. The DLA receiver also exhibits better performance than LRA in the low SNR regime, which is more obvious in the case of LLL-reduction with ZF. However, because LRA achieves the full diversity of the channel [173], the error rate in LRA eventually drops below that of the proposed algorithm. As expected, when the number hyperplanes that are explored decreases (i.e., smaller value of $\nu_{\max}$), the performance is degraded. However, the degradation is not significant for 2×2, 3×3, or even for 4×4 antennas when $\nu_{\max}$ is halved from $\nu_{\max} = 4$ to $\nu_{\max} = 2$. In Figure 3.17 it is seen that for 3×3 antennas, the SNR penalty only becomes noticeable when $\nu_{\max} = 1$.

The complexity involved in DLA is concentrated in the pre-processing stage that is only required each time the CSI is updated at the Rx. This involves solving a SVP via SD, which has complexity $\mathcal{O}(M^{\alpha N_T})$, as mentioned in section 3.5. However, once the USM are determined, DLA detection amounts to first computing the projections according to (3.61), and perform afterwards the matrix multiplications in (3.62), involving the Moore-Penrose inverse of the channel. Therefore, given that matrix multiplications have a number of operations (i.e., *complexity*) $\mathcal{O}(n^3)$ [195], which is the same as the complexity to compute the pseudo-inverse, the total number of operations is then bound by $2L\nu_{\max}\mathcal{O}(n^3)$, with $n = 2N_T$, because there are $2L\nu_{\max}$ candidates in (3.62) .

3.8 – Summary

This chapter began by providing some geometric and algebraic interpretations of the linear and SIC detection strategies. Then, the LRA receivers and the SD were introduced. Capitalising on some of the geometrical ideas shown previously, the chapter ends with the proposal of a receiver that takes advantage of a pre-processing stage based on the geometric relationships between the points in the primal lattice and the ones in the dual lattice. The receiver outperforms OSIC-ZF for the SER of interest and, in the very low SNR regime, outperforms LRA receivers. The proposed detection technique makes use of a "true sphere-decoder" that finds a set of successive minima in the dual lattice at the pre-processing stage. After that pre-processing, the subsequent symbol detection algorithm exclusively involves a linear transformation (using the pseudo-inverse matrix) in order to generate a list of candidate solutions for the underlying CVP. Because this computational burden is only needed when the channel changes, the receiver is suited for slow fading channels. This approach leads to significant gains in respect to OSIC for a reasonable number of candidates.

Chapter 4 – Exhaustive Search in Quantised Spaces

The optimal detection of symbols transmitted over a MIMO SM link was seen to be NP-hard in Chapter 2, and in Chapter 3 several sub-optimal approaches to the problem have been introduced. While MLD involves computing a number of Euclidean distances that grows exponentially with the dimension of a lattice, this does not restrain the use of exhaustive search when the number of points in the *finite* lattice is not too large.

This chapter proposes dividing the multidimensional Euclidean space into hypercubes by means of per-component quantisation, which enables a multiplication-free computation of the components of the squared Euclidean distances by means of a look-up table.

The proposed technique is particularly suitable for VLSI (very large scale integration) architectures and is inspired by similar problems in computer graphics and image processing where approximations[24] for the Euclidean distance have been used in [196] and [197] (although not for the *squared* Euclidean distance). The application of completely multiplication-free computation of Euclidean distances has been used in

[24] The approximation is also inspired by the type of simplifications that transform the forward-backward MAP algorithm into a max-log MAP algorithm in order to simplify implementation [249].

MIMO with minimum penalty [198], which applied approximations in the bidimensional space of the *transmit* constellation. Instead, this chapter shows the simplification of the evaluation of the Euclidean distances at the *receiver*. The key element in the proposed detection technique is a look-up table which was originally proposed to speed up the calculation of squared Euclidean distances in vector quantisation [199], [200].

4.1 – Quantised Spaces

Consider that $\mathbf{y}$ is the result of stacking the real and imaginary components of the received vector, according to the real equivalent model described in section 2.2.2. Denoting the quantisation process as $Q_\theta()$, the resulting quantised vector is

$$\left[\tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_{2N_R}\right]^T = Q_\theta\left(\left[y_1, y_2, \cdots, y_{2N_R}\right]^T\right). \tag{4.1}$$

In doing this, each one of these component $\tilde{y}_i \in \left\{c_1, c_2, c_3, \cdots, c_L,\right\}$, which correspond to the $\Theta = 2^b$ possible quantisation levels (i.e., described by b bits) with a uniform step size

$$q = c_i - c_{i+1}\,,\ i \in \left\{1, 2, \cdots, \Theta\right\}. \tag{4.2}$$

Now, one may denote as $\mathbf{y}^{(l)} = \mathbf{H}\mathbf{x}^{(l)}$ each one of the points in the real *finite* lattice. The Euclidean distances needed to solve (2.47) are then of the form

$$\left\|\mathbf{y} - \mathbf{y}^{(l)}\right\|^2 = \sum_{i=1}^{n}\left(\tilde{y}_i - \tilde{y}_i^{(l)}\right)^2,\ l{=}1,\ 2,\ \cdots,\ M^n\,. \tag{4.3}$$

For a particular lattice point $\tilde{\mathbf{y}}^{(l)}$, and defining $\Delta_i = \left(\tilde{y}_i - \tilde{y}_i^{(l)}\right)$, each particular squared Euclidean distance is

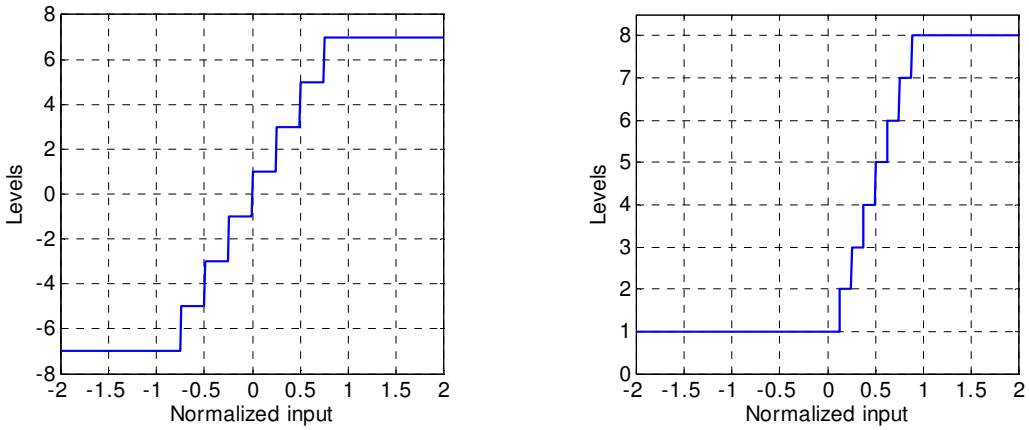
$$d^2 = \sum_{i=1}^{n}\Delta_i^2\,. \tag{4.4}$$

In [199] the authors considered a unitary increment, $q = 1$, and positive c_i, but in MIMO it is preferable to use

$$\left\{c_1, c_2, c_3, \cdots, c_\Theta,\right\} = \left\{-(\Theta-1), \cdots, -3, -1, +1, +3, \cdots, (\Theta-1)\right\}, \tag{4.5}$$

since each component of $\mathbf{y}^{(l)}$ can be either positive or negative, and $Q_\theta()$ needs to deal with both cases. Figure 4.1 (a) depicts the appropriate bipolar quantiser to be used in MIMO. It should be noted that both the received signal and the lattice itself can be bounded to $[-y_{i,sat}, +y_{i,sat}]$ in the i^{th} real dimension, corresponding to the clipping imposed by $Q_\theta()$. This maximum value could be $y_{i,sat} = \max\left\{y_i^{(l)}\right\}$ in each component and updated in each channel realization, however it is more convenient to make them all equal to $y_{sat} = \max\left\{y_i^{(l)}\right\}$ taken over all the real lattice points, i.e., l=1, 2, ···, M^n. This creates an hypercubic finite domain with edges having length $2y_{sat}$.

The look-up technique that will be presented in section 4.3 has been originally proposed in [199] for vector quantisation for the quantiser shown in Figure 4.1 (b). The use of such quantiser would require shifting all the lattice points by $y_{sat}/2$.



(a) Bipolar (b) Unipolar

Figure 4.1: Quantiser with $\Theta = 8$ levels ($b = 3$ bits) in each dimension normalising the input to y_{sat}.

4.2 – Quantisation Error

This section quantifies the effect of the quantisation described in section 4.1. The next sub-sections comment on the assumptions made in order to simplify the analysis and allow us to apply the analysis of scalar quantisers (e.g., [201]) to MIMO detection.

4.2.1 – Uncorrelated Noise and Uncorrelated Data

According to the system model in section 2.2.1, all data symbols are uncorrelated. Moreover, we assume that the quantisation noise, $\mathbf{n}_q$, is component-wise independent. These two assumptions allow the total variance (or power) of the *total noise* in a quantised vector to be written as

$$\sigma^2_{n_t} = \sigma^2_{n_q,1} + \sigma^2_{n_q,2} + \cdots + \sigma^2_{n_q,i} + \cdots + \sigma^2_{n_q,N_R} \,. \tag{4.6}$$

where $\sigma^2_{n_q,i}$ is the variance of the *quantisation noise* in the i^{th} (complex) dimension.

4.2.2 – Saturation Does not Impair Detection

The complex lattice of possible points in each receive antenna is a combination of N_T constellation symbols drawn from $\mathcal{A}_c$ weighted by the complex Gaussian channel matrix. If the hypercube with sides of length y_{sat} contains all the lattice points, then the *saturation noise* does not introduce any degradation in the ML problem. Consider the example in Figure 4.2, which shows the complex points received in each antenna of a 2×2 system using a traditional QPSK constellation and with the channel given by

$$\mathbf{H} = \begin{bmatrix} -0.3 + 0.5i & 0.3 - 0.2i \\ -0.6 + 2i & 1 + 2i \end{bmatrix}. \tag{4.7}$$

The effect of saturation will give rise to a quantised point in one of the faces of the hypercube. As can be seen in the 4 (real) dimensional case depicted in Figure 4.2, the closest lattice point can only lie at the intersection of the bounded subspace and the hypersphere D which is the projection of $\mathbf{y}$ in the side of the hypercube that is closer to it. So, the original k^{th} distance can be expressed in terms of the distance to the projection and the remaining k^{th} distance $\mathbf{b}_k$: $\mathbf{d}_{\text{k}} = (\tilde{\mathbf{y}} - \mathbf{y}) + \mathbf{b}_k$. Because $(\tilde{\mathbf{y}} - \mathbf{y})$ is fixed and it is impossible to have a lattice point inside region C, then minimizing $\mathbf{d}_k$ or $\mathbf{b}_k$ yields the same solution.

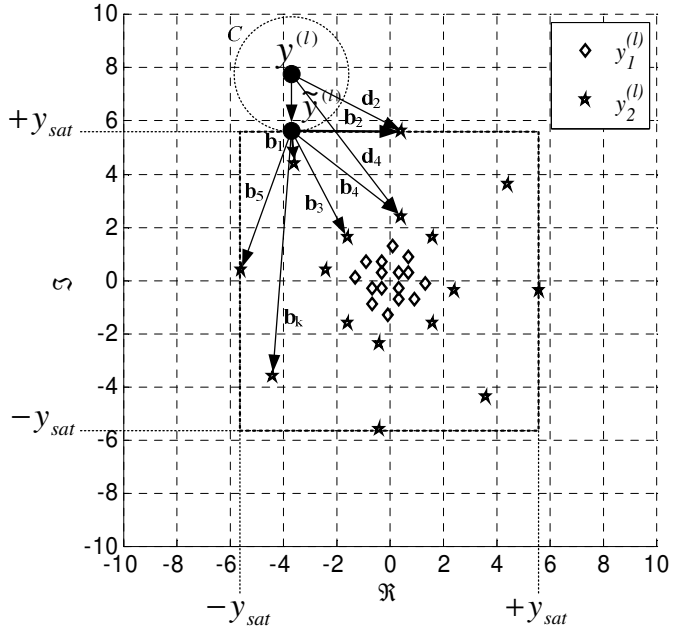


Figure 4.2: The two components of the *complex* lattice of a 2×2 system with QPSK symbols ($M^{N_T} = 16$).

4.2.3 – Uniform Error Per Component

Considering that errors coming from saturation are negligible (assumption 4.2.2), the only cause of degradation in the performance will be the granular noise. Considering that the quantisation in each dimension is described by a uniform error distribution, it is straightforward to obtain the well known expression for the quantisation noise power (e.g., [201])

$$\sigma_q^2 = \int_{-q/2}^{q/2} \frac{1}{q} x^2 dx = \frac{q^2}{12}. \tag{4.8}$$

Independently of the number of dimensions, n, the mean error per dimension was obtained by simulation using

$$E\left\{n_q\right\}_{[\%]} = E\left\{\left|1 - \frac{\left\|\tilde{\mathbf{y}} - \tilde{\mathbf{y}}^{(l)}\right\|^2 - \left\|\mathbf{y} - \mathbf{y}^{(l)}\right\|^2}{\left\|\mathbf{y} - \mathbf{y}^{(l)}\right\|^2}\right|\right\} \cdot 100 \tag{4.9}$$

and the result is shown in Figure 4.3.

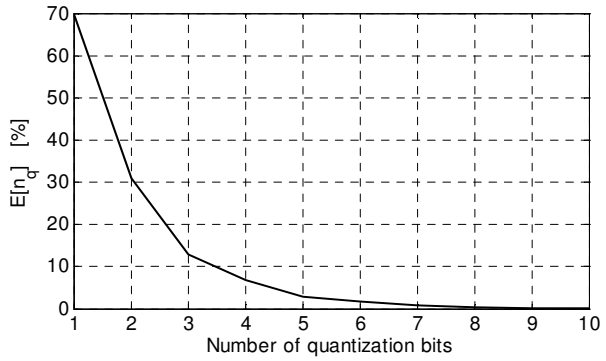


Figure 4.3: Quantisation error for the squared Euclidean distance as a function of the number of quantisation bits, b , obtained by simulation.

Using (4.6) and (4.8), the signal to total quantisation noise ratio is obtained by

$$\frac{\sigma_x^2}{\sigma_{n_{total}}^2} = \frac{\sigma_x^2}{\sigma_{n_q}^2} = \frac{\sigma_x^2}{\sum_{i=1}^{n} \frac{q_i^2}{12}} = \frac{\sigma_x^2}{\sum_{i=1}^{n} \frac{\left(2y_{i,sat}/\Theta\right)^2}{12}} = \frac{3\Theta^2\sigma_x^2}{\sum_{i=1}^{n} y_{i,sat}^2}. \tag{4.10}$$

4.2.4 – Equal Saturation in the Dimensions (hypercube)

When $y_{i,sat}$ is set to the same value in all of the n dimensions, (4.10) yields

$$\frac{\sigma_x^2}{\sigma_{n_q}^2} = \frac{3\Theta^2\sigma_x^2}{ny_{sat}^2} = 3 \cdot \frac{(2^b)^2}{n} \cdot \left(\frac{\sigma_x}{y_{sat}}\right)^2. \tag{4.11}$$

or, equivalently,

$$\left(\frac{\sigma_x^2}{\sigma_{n_q}^2}\right)_{dB} = 4.77 + 6.02b - 10\log_{10}(\underbrace{2N_R}_{=n}) + 20\log_{10}\left(\frac{\sigma_x}{y_{sat}}\right). \tag{4.12}$$

Expression (4.12) shows that when N_R doubles the quantisation noise increases by 3 dB. On the other hand, every extra bit used in the quantisation of each component improves the signal-to-quantisation noise on that real component by 6 dB. Thus, when increasing the number of antennas from 2 to 4, only 0.5 extra bits would be necessary to compensate the loss. Figure 4.4 shows the trade-off arising from $6.02b = 10\log\left(n\right)$.

A second outcome from (4.12) is that its final term implies that use of an equal value of y_{sat} will lead to, as expected, a poor performance in the antennas having a "more compact" received constellation. Indeed, Figure 4.2 shows an example of that: the total power in the first row of (4.7) leads to a much more geometrically "compact" received constellation in first receive antenna, i.e., $E\left\{ (y_1^{(l)})^2 \right\} << E\left\{ (y_2^{(l)})^2 \right\}$.

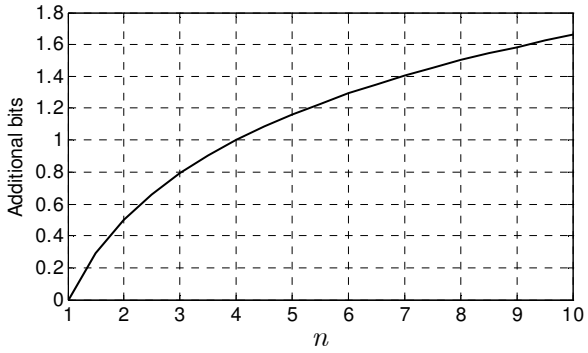


Figure 4.4: Additional bits required to compensate the loss associated with more dimensions in the lattice.

4.3 – The Look-Up Table Technique

All the possible values of the distance components Δ_i^2 in (4.4) correspond to one particular element of the matrix

$$\Xi^{(1)} = \begin{bmatrix} (c_1 - c_1)^2 & (c_1 - c_2)^2 & (c_1 - c_3)^2 & \cdots & (c_1 - c_\Theta)^2 \\ (c_2 - c_1)^2 & (c_2 - c_2)^2 & (c_2 - c_3)^2 & \cdots & (c_2 - c_\Theta)^2 \\ (c_3 - c_1)^2 & (c_3 - c_2)^2 & (c_3 - c_3)^2 & \cdots & (c_3 - c_\Theta)^2 \\ (c_4 - c_1)^2 & (c_4 - c_2)^2 & (c_4 - c_3)^2 & \cdots & (c_4 - c_\Theta)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_\Theta - c_1)^2 & (c_\Theta - c_2)^2 & (c_\Theta - c_3)^2 & \cdots & (c_\Theta - c_\Theta)^2 \end{bmatrix}. \tag{4.13}$$

An inspection of $\Xi^{(1)}$ allows us to notice its expected symmetry and, furthermore, that it is possible to re-write it as

$$\Xi^{(2)} = \begin{bmatrix} 0 & (c_1)^2 & (c_2)^2 & \cdots & (c_{\Theta-1})^2 \\ (c_1)^2 & 0 & (c_1)^2 & \cdots & (c_{\Theta-2})^2 \\ (c_2)^2 & (c_1)^2 & 0 & \cdots & (c_{\Theta-3})^2 \\ (c_3)^2 & (c_2)^2 & (c_1)^2 & \cdots & (c_{\Theta-4})^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (c_{\Theta-1})^2 & (c_{\Theta-2})^2 & (c_{\Theta-3})^2 & \cdots & 0 \end{bmatrix}. \tag{4.14}$$

The elements of this matrix can be seen to be associated with the values of the quantisation levels by $\Xi^{(2)}_{m,n} = (c_{|m-n|})^2$. Moreover, all the entries in $\Xi^{(2)}$ (i.e., all the squared distance components) belong to the ordered set

$$\Xi = \left[0, (c_1)^2, (c_2)^2, (c_3)^2, \cdots, (c_{\Theta-2})^2, (c_{\Theta-1})^2\right]^T. \tag{4.15}$$

Using the following rule,

$$\Xi^{(1)}_{m,n} = \Xi^{(2)}_{m,n} = \Xi(a), \quad \text{with } a = \left(\frac{|c_m - c_n|}{q} + 1\right), \tag{4.16}$$

it is possible to locate and read the value of the distance component Δ_i^2 from the values pre-stored in Ξ. Observe also that the division by q in (4.16) converts the absolute separation between components to the integer number of intervals between the two of them.

The use of this *non-truncated* look-up table does not introduce any errors in addition to the ones described in section 4.2 because it is an exact method in the quantised space. The authors of [199] and [200], proposed a *truncated* table to replace Ξ, however this would not be useful in the context of MIMO detection.

4.4 – Simulation Results

Simulation results for the receiver using maximum likelihood in a quantised space (MLQS) are presented in Figures 4.5 to 4.8 for different systems using the low order modulations QPSK and 16-QAM in the various symmetric antenna configurations (i.e., with $N_T = N_R$). All figures include the performance of the proposed receiver for different values of the number of bits per component and also the performances

obtained using ZF, MMSE and OSIC (with ZF or MMSE criterion) as well as the performance of MLD. It is worth mentioning that, contrary to all the results presented in other chapters, the OSIC receiver implemented in this chapter works directly with the complex constellations and not with the real equivalent model presented in section 2.2.2 and for that reason its performance is slightly degraded in comparison to those. This last effect is known in the literature [95] (sec. 4.3.3), and is related with the fact that in the real model SIC is performed independently in the real and imaginary components. This de-coupling (which doubles the lattice dimension) leads to less error propagation when deciding for complex symbols.

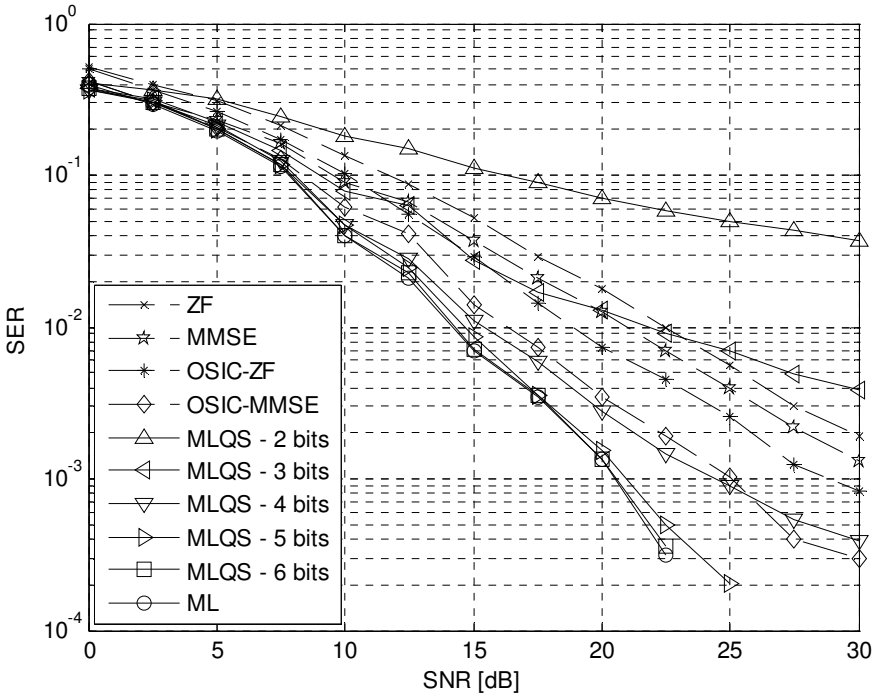


Figure 4.5: Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 2×2 system using QPSK modulation.

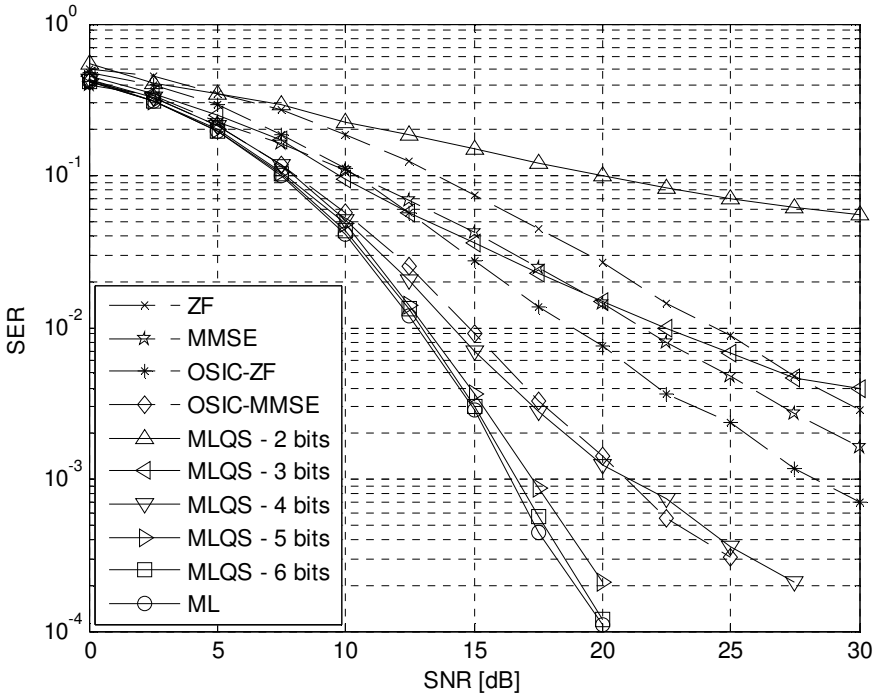


Figure 4.6: Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 3×3 system using QPSK modulation.

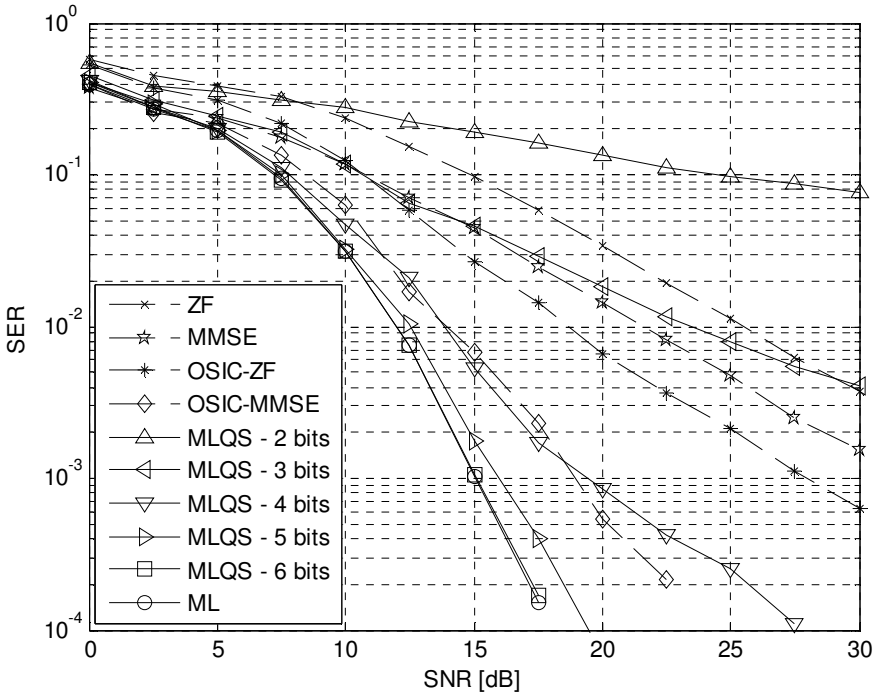


Figure 4.7: Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 4×4 system using QPSK modulation.

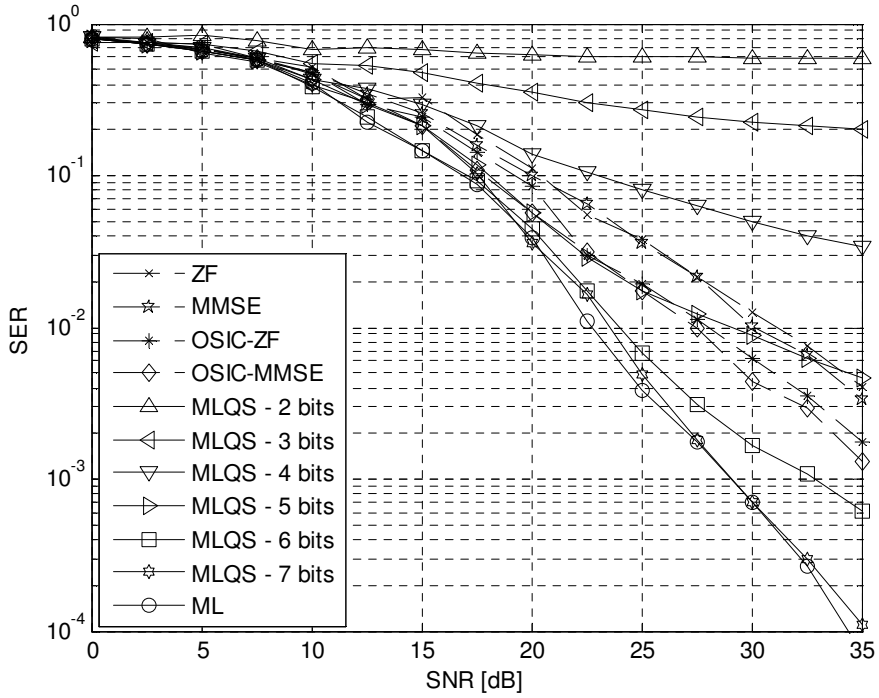


Figure 4.8: Performance for standard receivers and detection in a quantised space for different levels of quantisation per dimension in a 2×2 system using 16-QAM.

The results of the simulations for the traditional receivers (ZF, MMSE, OSIC-ZF, OSIC-MMSE, and ML) were validated against other results available in the literature: for QPSK with 2×2 antennas, the traditional receivers and ML can be compared with the ones in [68]; for QPSK with 4×4 antennas results can be found in [95] ; and the results for 16-QAM with 2×2 antennas are available in [202].

The effect of Gaussian noise should be added to the quantisation noise. As they are independent, the effective noise power is given by summing the respective noise powers. Consequently, the overall SNR is

$$\left(\frac{\sigma_x^2}{\sigma_{n_t}^2}\right)^{-1} = \left(\frac{\sigma_x^2}{\sigma_{n_g}^2}\right)^{-1} + \left(\frac{\sigma_x^2}{\sigma_{n_q}^2}\right)^{-1} \quad \Leftrightarrow \quad \left(\frac{\sigma_x^2}{\sigma_{n_t}^2}\right) = \frac{\left(\frac{\sigma_x^2}{\sigma_{n_g}^2}\right) \cdot \left(\frac{\sigma_x^2}{\sigma_{n_q}^2}\right)}{\left(\frac{\sigma_x^2}{\sigma_{n_g}^2}\right) + \left(\frac{\sigma_x^2}{\sigma_{n_q}^2}\right)}. \tag{4.17}$$

A consequence of this relationship is that the overall SNR is always limited by the partial SNRs:

$$\left(\frac{\sigma_x^2}{\sigma_{n_t}^2}\right) \leq \min\left\{\left(\frac{\sigma_x^2}{\sigma_{n_g}^2}\right), \left(\frac{\sigma_x^2}{\sigma_{n_q}^2}\right)\right\}. \tag{4.18}$$

For this reason, this *effective* SNR may be limited by the quantisation error, which is a function of both the lattice and of the number of bits per dimension, b, as seen in (4.12). On average, and independently of the transmission scheme, one can observe that as the number of quantisation levels b increases, the SER converges to its lower bound, limited by the existence of the Gaussian noise.

The results with QPSK show that for b=2 the SER is worse than that for any other receiver analysed; for b=3 it is close to the performance of ZF; for b=4 it is similar to the performance of OSIC-MMSE; for b=5 it is always within 1 dB of ML; and for b=6 it always coincides with ML. These results show that the total number of bits needed to accurately represent the n-dimensional received vector is $5\times(2\times N_R)$, i.e., for the most demanding case considered (4×4, where there are 4^4=256 possible points in the lattice), 40 bits are needed to obtain near ML performance.

The number of bits needed to represent both the received vectors and the lattice associated with each channel realization is shown to be small, however it could be further reduced by quantising with independent saturation limits for each component. Additionally, the number of required pre-stored components constitutes a very small table with only Θ positions.

Note that the simplified analysis that has been presented suffices to understand the impact of the quantisation shown in the simulations: doubling the number of antennas from 2 to 4 imposes a power loss that can be more than compensated by increasing the number of bits per dimension from 5 to 6. Indeed, inspecting the cases depicted in Figures 4.5 and 4.6, and measuring the difference of energy at an SER=10^{-3}, the correct number of additional bits required to maintain performance can be seen to be the predicted "half bit". In MIMO systems that do not go beyond 4 antennas at each side,

the need for a 6^{th} quantisation with QPSK should not be required. However, for an identical number of lattice points in each dimension (16^2=256), the use of 16-QAM requires a greater number of quantisation bits than does QPSK because there are more coordinates to be distinguished per dimension. The benefits of quantisation are more clear when low order modulations are used, i.e., QPSK and 16-QAM (or their one-dimensional counterparts with amplitude shift keying: 2-ASK and 4-ASK).

4.5 – Summary

This chapter presents a technique to simplify the calculation of the squared Euclidean distances required when a MLD-based approach to CVP is still possible (i.e., for low order modulations with a small number of antennas). The detection problem is sub-optimally solved after quantising the received vector. Then, a look-up table with pre-stored components provides the distance metrics. The number of pre-stored elements can be made as small as the number of quantisation levels per dimension. This procedure eliminates the multiplications involved in the calculation of the squared Euclidean distances. The number of comparisons needed remains exponential with the number of transmits antennas; however, the total complexity required is reduced by replacing multiplications [198] with readings from a look-up table [199], [200].

Chapter 5 – Alternative Representations of Lattices

"At one time they thought that the travelling salesman problem might fit the bill, since they were told by mathematicians that it was NP complete. However, it turned out that algorithms exist which yield approximate solutions of sufficient accuracy for all practical purposes. Non-mathematicians should be careful how they interpret what mathematicians tell them!"

Sir Maurice V. Wilkes, *Moore's law and the future*,
Computer Laboratory Seminar, Oct. 2002, transcript in [203].

This chapter is an *intermezzo* that focuses on alternative representations of lattices that permit us to specify a lattice using less bits than are required in the conventional representation using a $n \times n$ matrix. Such representations could be beneficial to the reduction of the amount of data needed to be fedback from the receiver to the transmitter in order to provide CSIT in closed loop links. Two different representations of lattices will be presented, which have been developed in the field of algorithmic number theory and which have application in cryptography, while remaining largely ignored in the MIMO literature.

Since the Hermite normal form (HNF) is upper triangular (u.t.) and is often sparse, some authors have questioned if the use of the HNF could be used as a means to

simplify the traversal of the tree in SD [204], [205] (p.26). That question has not yet been answered until now, probably owing to the problems related with the implementation of the HNF.

5.1 — The Hermit Normal Form

As was mentioned in Chapter 2, there are an infinite number of different bases representing the same lattice. The literature on cryptography traditionally highlights that any lattice basis can be changed into the Hermite normal form (HNF) by means of unimodular transformations. A lattice generator matrix can be brought to a triangular form, with all entries positive and strictly smaller than the diagonal. The HNF form exists for both integer and rational matrices [109], and is obtained by means of elementary operations on the lattice, that is:

$$\mathbf{H}_{\mathrm{HNF}} = \mathbf{H} \cdot \mathbf{M}\,, \tag{5.1}$$

with $\mathbf{M}$ unimodular. Most importantly, the HNF of a basis of a lattice is *unique* (not considering rotations of the lattice).

Some literature on algorithmic number theory reminds us that HNF also exists and is unique for rational lattices as well. However, the computation in the rational case is always said to be the same as for an integer matrix, if one previously scales the rational basis by the greatest common divisor of all elements in the generator matrix. The argument is true, however one must be aware that this method may easily lead to very large numbers in practical applications, even for a moderate number of dimensions. Sadly, the computation of HNF has not yet been properly dealt with in the literature, as Sims warns his readers in the preface to his book [206]: *"It is not usual for an author of a mathematics text to make evaluative judgments concerning the works in the Bibliography, and I have agonized over my decision to break with this practice. However, I feel an obligation to the reader to state my opinion that the quality of the papers dealing with the computation of Hermite and Smith normal forms is on average noticeably below the level in the other works cited. In a significant number of these*

papers there are deficiencies in the exposition and even in the validity of the arguments."

In addition to that, even the definition and the name itself of the HNF is not consistent across the literature (e.g., [136]), as it is sometimes called (row or column) *echelon form* or even *integer normal form* [112].

Ironically, Sims presentation of the algorithm in [206] (sec. 8.5) is also much criticised in [207] (p.23). The author included a section entitled "obscurity in the algorithm", commenting on Sims's presentation of HNF. Some of the comments are: *"Sims just adumbrated a method to compute Hermite normal form. There are certain areas in the algorithm that needs some light to be thrown on. (...) The algorithm does not throw light on how the pivots must be chosen. (...) Lines 6 and 12 of the algorithm describe a division operation but again the algorithm does not describe what the division is. The algorithm nonplusses the reader on obtaining the quotient of a non-positive division or even a normal division with a non-zero remainder".*

Despite the criticism, The Kannan-Bachen algorithm [208], in the form given by Sims in [206] (sec. 8.5) is the most simple and detailed algorithm available in the literature. The problems that it raises have been solved and it was implemented in MATLAB® as given in Algorithm 5.1.

Notice that the algorithm given by Sims requires full-rank matrices. Algorithm 5.1 is also applicable to rank-deficient matrices, such as the one in the following example,

$$\begin{bmatrix} 2 & 2 & -1 & 0 \\ -2 & 2 & 1 & 0 \\ -2 & 0 & 2 & -2 \\ -1 & 1 & 0 & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 2 & 3 & -1 & 0 \end{bmatrix}}_{\text{HNF}} \cdot \underbrace{\begin{bmatrix} -1 & -2 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & -2 & 0 & 2 \\ 0 & 0 & -1 & 1 \end{bmatrix}}_{\text{M}}, \tag{5.2}$$

where the zero element in the diagonal denotes implies that the determinant is zero and therefore the matrix in indeed rank-deficient. Indeed, the fact that the HNF includes one column containing just zeros, indicates that the remaining three non-zero generators suffice to span the whole lattice.

ALGORITHM 5.1: HNF ALGORITHM (KANNAN-BACHEN)

```
function [A_hnf M]=HNF(A)

A_orig=A;
m=size(A,1);
n=size(A,2);

s=n; % s is the index of the last non-zero column of A

j=1;
sigma=1:n;
M=eye(n); % sets the unimodular matrix to identity

while j<=s
    %This if is for the square part, so the column index only
    % increases towards the row index

    for i=1:j-1
        [g c d]=gcd(A(i,i),A(i,j));
        MM=[c, -A(i,j)/g;...
            d, A(i,i)/g]; % updating the unimodular matrix
        A_aux=A(:,[i j])*MM;

        M_aux=eye(n);
        M_aux(i,i)=c;
        M_aux(j,i)=d;
        M_aux(i,j)=-A(i,j)/g;
        M_aux(j,j)=A(i,i)/g;

        M=M*M_aux;

        %Copy the 2-columns into the appropriate columns of A
        A(:,[i j])=A_aux;
        reduce(i); %Reduces all the elements to the left of A_ii
    end

    col_with_nonzero=min(find(A(:,j)));

    if isequal(A(:,j),zeros(size(A(:,j))))
        %Swap last non-zero column with the one found to be zero
        A(:,[j,s])=A(:,[s,j]);
        M(:,[j,s])=M(:,[s,j]);
        s=s-1
    elseif col_with_nonzero~=j
        row_with_nonzero=min(find(A(j,j+1:end)))+j
        if isempty(row_with_nonzero)
          %Find in the "minor to the right of row j" one column with
          %at least one non-zero element
          row_with_nonzero=find(sum(abs(A(1:j,j+1:end))))+j
          A(:,[j,row_with_nonzero])=A(:,[row_with_nonzero,j]);
          M(:,[j,row_with_nonzero])=M(:,[row_with_nonzero,j]);
        else
            A(:,[j,row_with_nonzero])=A(:,[row_with_nonzero,j]);
            M(:,[j,row_with_nonzero])=M(:,[row_with_nonzero,j]);
        end
    else
```

```
        reduce(j);
        j=j+1;
        end
    end

    A_hnf=A;

        function reduce (k) % (a nested function)

            if A(k,k)<0
                A(:,k)=-A(:,k);
                M(:,k)=-M(:,k);
            end
            for z=1:k-1
                reduction=floor(A(k,z)/A(k,k));
                M_aux=eye(n);
                M_aux(k,z)=-reduction;
                M=M*M_aux;
                A(:,z)=A(:,z)-reduction*A(:,k);
            end
         end
end
```

The computation of the HNF using Algorithm 5.1 was tested for numerous Gaussian random matrices and it was concluded that the HNF for matrices larger than 4×4 almost always leads to matrices with too large entries, which makes the storage of the HNF impracticable. This is not a feature dependent on the algorithm used to compute the HNF, but is rather related with the definition of the HNF itself.

5.2 — Representation by a Modular Equation

Since lattices are additive (or Abelian) groups [206] (p. 320), their study is closely related with group theory, [109], [209]. One starts by noting that particular integer lattices have a coset structure, which means that they can be written in the form

$$\Lambda = \Lambda' + \left[\frac{\Lambda}{\Lambda'}\right], \tag{5.3}$$

where $\left[\Lambda \,/\, \Lambda'\right]$ is a *system of coset representatives* for the elements of the *quotient group* $\Lambda \,/\, \Lambda'$. The underlying geometry is that Λ' is a sublattice of Λ and that sublattice defines its own fundamental region, which is not restricted to being of any particular shape. The number of lattice points lying inside the fundamental region of

the sublattice is called the *index* of the sublattice. The term $\left[\Lambda / \Lambda'\right]$ consists of a finite set of lattice points, each one representing family of lattice points that constitute an *equivalent class* defined by an *equivalence relation* [206] (p.7) . The lattice points in each of those families all share the same property: any point is related with another member of family by adding some particular vector of the sublattice Λ' . This constitutes a generalisation of the concept of the modulo operation defined in $\mathbb{Z}$. In fact, members of an equivalent class are said to be *equivalent modulo* Λ' .

Because $\mathbb{Z}^n$ is also a lattice, one can define the quotient group $\mathbb{Z}^n / \Lambda$ for some integer lattice Λ . Some of these quotient groups have the so called cycle property and therefore can be written in the form [137]

$$\mathbb{Z}^n / \Lambda \sim \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_t} \tag{5.4}$$

and k_i divides k_{i+1} for $i = 1,2,\ldots,t-1$. t is called the *number of cycles* of the lattice.

Expression (5.4) indicates that each point in Λ can be written as a Cartesian product of coordinates that, in each dimension i belong to an equivalence class of $\mathbb{Z}$ modulo k_i . In other words, there is just a finite number of non-equivalent coordinates that any point in Λ can take. It is important to note that, for simplification, it is usual to take as coset representatives the points inside the fundamental region of Λ , as defined in (2.2) in Chapter 2.

Moreover, it is can be proven that a lattice with cycles can be entirely defined by a set of d *modular linear equations* and all points in the lattice constitute the solutions to those equations:

$$\Lambda = \left\{ \mathbf{y} : \left\langle \mathbf{u}_1, \mathbf{y} \right\rangle = 0 \bmod k_1 \wedge \left\langle \mathbf{u}_2, \mathbf{y} \right\rangle = 0 \bmod k_2 \wedge \cdots \left\langle \mathbf{u}_d, \mathbf{y} \right\rangle = 0 \bmod k_m \right\} \tag{5.5}$$

Trolin has shown in [137] that any lattice can be well approximated by a lattice possessing a cycle structure such as the one of (5.4). The limit case where $t = 1$ is of most interest because it implies that an n-dimensional lattice can be entirely specified by just one modular equation. Those lattices are called *cyclic lattices*.

Intuitively, a lattice Λ' is geometrically close to the lattice Λ if their points are close to each other in a one to one correspondence. However, notice that a lattice with

a small offset added to all its points is no longer a lattice as it would not contain the origin. It is useful to define the concept in terms of the generator matrix of the two lattices:

A $(\mathbf{H},\varepsilon)$-*neighbourhood* of a lattice defined by the matrix generator $\mathbf{H}$ consists of the lattices generated by the matrices $\mathbf{H}'$ for which [210] (p.11)

$$\left\|\mathbf{H},\varepsilon\right\| \triangleq \max_{i,j}\{\mid h_{ij} - h'_{ij} \mid\} < \varepsilon\,, \tag{5.6}$$

where ε is an arbitrary positive real number.

One other interesting result, proven by Paz and Schnorr in [136], is that any integer lattice can be approximated by a cyclic lattice, i.e., be specified by a single modular equation. This could be of much interest to represent the lattice associated to a particular channel realisation and therefore eliminate the need to feedback all the complex coefficients of the channel matrix. That would do away with the omnipresent generator matrix in the MIMO literature.

As defined in [136], let $\sigma : \Lambda \to \mathbb{Z}^n$ be a linear transformation and k an integer scaling factor k. It can be shown that these two properties hold:

i) $\left\|\mathbf{y} - \dfrac{\sigma(\mathbf{y})}{k}\right\| \le \varepsilon \left\|\mathbf{x}\right\|$, for all $\mathbf{y} \in \Lambda$;

ii) the quotient group $\dfrac{\mathbb{Z}^n}{\sigma(\Lambda)}$ is cyclic.

Then, given some integer lattice Λ, the construction of a nearby cyclic lattice takes the generator matrix of Λ and slightly perturbs its generator vectors by the linear mapping $\sigma(\Lambda)$. The procedure is split into two different cases but in both the type of operations encountered is similar. For the purpose of the argument here, it suffices to show just one of the cases. In the simplest case, each element of $\mathbf{H}$ must be perturbed according to

$$\frac{\sigma(\mathbf{h}_i)}{k} = \tilde{\mathbf{h}}_i = \left[\mathbf{h}_{i1}, \mathbf{h}_{i1}, \cdots, \mathbf{h}_{in}\right] \tag{5.7}$$

$$\tilde{h}_{ij} = \begin{cases} h_{ij} & ,\text{if i} \neq \text{j} \\ h_{ii} - \dfrac{1}{k}, & ,\text{if i} = \text{j}\,. \end{cases} \tag{5.8}$$

Hence, the approximation takes place in the integer domain, after having scaled $\Lambda(\mathbf{H})$ by k. Paz and Schnorr prove that this scaling factor should be

$$k \triangleq \left\lceil \frac{1}{\varepsilon} \right\rceil 2^n \prod_{i \neq j} \left| h_{ii} - h_{jj} \right|. \tag{5.9}$$

Even for a moderate number of dimensions (in the real equivalent model), (5.9) leads to extremely large values of k.

The approach by Trolin [137] to prove that any lattice can be approximated in a similar manner by a lattice with t cycles provides an alternative way for constructing a cyclic lattice. It can be proven that all cyclic lattices have a basis whose HNF is of the form

$$\mathbf{H}_{\text{HNF}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & 0 \\ h_{n,1} & h_{n,2} & \cdots & h_{n,n-1} & t \end{bmatrix}. \tag{5.10}$$

Moreover, it is not difficult to prove that any basis that has already been brought to HNF can also be reduced to the form of (5.10). For this purpose, consider a matrix in HNF,

$$\mathbf{H}_{\text{HNF}} = \begin{bmatrix} h_{1,1} & & & & & \\ h_{2,2} & h_{2,2} & & & \mathbf{0} & \\ h_{3,3} & h_{3,2} & h_{3,3} & & & \\ \vdots & \vdots & \vdots & \ddots & & \\ h_{n-1,1} & h_{n-1,2} & h_{n-1,3} & & h_{n-1,n-1} & \\ h_{n,1} & h_{n,2} & h_{n,3} & \cdots & h_{n,n-1} & h_{n,n} \end{bmatrix}, \tag{5.11}$$

and now (5.11) is perturbed inserting $n-1$ ones in the following positions:

$$\tilde{\mathbf{H}}_{\text{HNF}} = \begin{bmatrix} h_{1,1} & 1 & & & & \\ h_{2,2} & h_{2,2} & 1 & & \mathbf{0} & \\ h_{3,3} & h_{3,2} & h_{3,3} & 1 & & \\ \vdots & \vdots & \vdots & \ddots & 1 & \\ h_{n-1,1} & h_{n-1,2} & h_{n-1,3} & & h_{n-1,n-1} & 1 \\ h_{n,1} & h_{n,2} & h_{n,3} & \cdots & h_{n,n-1} & h_{n,n} \end{bmatrix}. \tag{5.12}$$

If one takes the leftmost column and place it at the right of the remaining matrix, the matrix immediately becomes u.t except for the last column on the right. Then, one can cancel all the elements in that rightmost column with the ones in the main diagonal. Finally, all the off-diagonal elements can also be brought to zero taking advantage of the ones in the diagonal. Note that all these operations are elementary matrix transformations as the ones in section 2.1.2, and therefore the underlying lattice remains unchanged. The end result is a matrix in the form (5.10), where the only non zero elements are the ones in the diagonal and the last row (which are last coordinates of the generator vectors).

This result is of enormous practical relevance as it provides a tool not only to discover if a lattice has one cycle (i.e., is a cyclic lattice) but also construct a synthetic cyclic lattice nearby any given lattice, just by perturbing its HNF in a straightforward manner.

Notice that the solution to the CVP when the lattice is written in the from (5.10), can be calculated in one-shot by

$$y \begin{cases} x(1) = y(1) \\ x(2) = y(2) \\ \quad \vdots \\ x(n-2) = y(n-2) \\ x(n-1) = y(n-1) \\ y_n = \dfrac{y(n) - h_{n,1}y(1) - h_{n,2}y(2) - \cdots - y(n-1)h_{n,n-1}}{t} \, . \end{cases} \tag{5.13}$$

Such a receiver has been implemented and its performance accessed with MIMO Gaussian matrices previously scaled so that the change from 0 to 1 in (5.12) would not significantly change the lattice. However, one should notice that a basis in HNF (such as the one in (5.10)), provides an extremely poor coverage of the Voronoi region. Several simulations have been run for the technique described in (5.13) and the performance was seen to be coincident with that of the ZF receiver. The reason for that is the error propagation in the first $n-1$ layers in (5.13).

5.3 — Summary

This semitutorial chapter described how some particular geometrical and algebraic structures in some families of lattices enable a shorter presentation of a lattice than the one provided by the traditional generator matrix. The chapter shows that the nature of these representations favours the representation of intege lattices and huge numerical difficulties are encountered when they are applied to rational lattices, such as the ones arising in MIMO radio channels. Even though rational lattices can always be scaled to integers ones, some of its algebraic properties are deeply connected with the determinant of the lattice or with the magnitude of the coordinates and scaling rational lattices to integers brings up severe numerical problems.

The HNF of a lattice was first presented. Then, it was shown that integer lattices may be well defined by a single modular equation.

One important idea introduced in this chapter is that of approximating one lattice by another lattice in its neighbourhood while that second lattice has some specific property. This idea will be further explored in the next chapter.

Chapter 6 – Focusing Onto Orthogonal Quotient Groups

In the previous chapter it was shown that some properties, representations or tools that are useful for integer lattices, unfortunately face tremendous limitations if applied in the MIMO context. The reason is that the lattices in MIMO neither have integer entries nor have determinants exceptionally small (in which case the computation of the HNF would not be troublesome). This chapter explores an idea, rooted in group theory, that opens doors to a new type of receiver by slightly relaxing the accuracy of the representation of the lattices. The idea is to linearly transform (to *focus*) the received lattice onto another lattice, which can be expressed as the union of translates of a rectangular sublattice. This allows mapping the detection problem onto a trellis.

6.1 – Lattices with a Trellis Representation

It has been known since the late 80's that some lattices have a trellis representation and this fact was not forgotten by Agrell et al. in their semi-tutorial paper [106]. Nevertheless they dismiss the practicality of that representation because the complexity of the trellis (usually measured as the number of paths) is known to grow exponentially with the number of dimensions [211], [212]. While that argument is valid, it could also be applied to sphere decoding. Even so, because the typical number of antennas in MIMO is rather small (in comparison to hundreds of dimensions required in

cryptographic applications, e.g., [213]), sphere decoding is considered a practicable quasi-optimum detection algorithm. One more important difficulty is that lattices with a trellis representation require very particular geometries that are not found in lattices randomly generated. In this chapter we show that for the typical number of dimensions used in MIMO communication, with high probability, there exists a "synthetic" lattice that is a member of the family of lattices that have a trellis representation and which is sufficiently close to any given random lattice. For this purpose a method will be presented to find a trellis-oriented basis for a given random lattice.

The pioneering work by Forney [117], [214], and by Calderbank and Sloan [215], showed that some lattices can be described by a trellis, where each segment of the trellis is associated with the coordinates of the lattice points in each dimension of the space. This work was related with that on *group codes* or (*codes on groups*) and was fundamental to the development of trellises for block codes [6], [216], [9], [10]. Soon, practical implementations for lattice decoding using trellises emerged [217] (and references therein).

The lattices for which a trellis exists, can be said to constitute a *family* of lattices, denoted by $\mathcal{L}_R$. Unfortunately, the existence of a trellis representation requires a rather restricted type of lattice. Some well known lattices belong to $\mathcal{L}_R$; examples of these are the hexagonal lattice in 2D, the Schläfli lattice in 4D, the Gosset lattice in 8D (respectively denoted by A_2, D_4, and E_8), or the Leech lattice in $\mathbb{R}^{24}$ [20]. Many others exist and can be constructed by imposing a specific geometrical structure during the design of the code (perhaps the most comprehensive description is the one in [210]). In those cases MLD can be attained by means of trellis detection, and therefore the CVP in these cases can be solved with the Viterbi algorithm. By performing the detection on a trellis one may circumvent the exponential complexity of MLD (measuring the distance from the given point to all the points in the lattice), while keeping its performance.

Clearly, the trellis detection approach cannot be extended to any random lattice. However, one may ask the question, for any given lattice, can one find a lattice that is

sufficiently "similar" or "close" to it, and yet is simultaneously a member of the family of lattices with a trellis representation, $\mathcal{L}_R$? This is the main question dealt with in this chapter. As lattices are defined by generator matrices, the problem can be seen as a *matrix nearness problem* [144]; as in many other matrix nearness problems, the one we formulate also does not seem to have an analytical solution and therefore we take an algorithmic approach.

The approximation of a random lattice by a lattice in $\mathcal{L}_R$ is a novel approach to MIMO detection. While the use of a trellis structure appears in [218], that approach is clearly sub-optimal, as it is based on a transformation of a tree structure into a trellis structure, by "folding" and merging branches onto other branches, and eventually losing information to distinguish lattice points.

6.2 — Focusing Onto Lattice Sets

We call $\mathcal{M}$ the set of all possible lattices in $\mathbb{R}^n$. Hence, $\mathbb{Z}^n$ is just one particular lattice in $\mathcal{M}$ (see Figure 6.1). Moreover, all lattices with a trellis representation are also members of that $\mathcal{M}$ and, as mentioned in section 6.1, we say that they constitute the $\mathcal{L}_{\mathrm{R}}$ family of lattices.

As it was described in Chapter 3, the simplest way of solving the CVP amounts to the least-squares solution given by the Moore-Penrose pseudo-inverse of the generator matrix, i.e., the ZF solution. Geometrically, this type of linear receiver applies a linear transformation that takes the received lattice Λ and transforms it back into the original $\mathbb{Z}^n$. One may generalise this concept and call this procedure a *focusing* of the received lattice Λ onto $\mathbb{Z}^n$. One may generalize this concept of focusing one lattice onto some other lattice by means of some linear transformation $\mathcal{F}$. The ZF focusing approach presents the lowest complexity among all sub-optimal receivers but also results in the poorest performance (in terms of erroneous decisions). The poor performance is a direct consequence of the potentially huge mismatch between the optimal decision regions in MLD and the decision regions associated with focusing onto

$\mathbb{Z}^n$. These decision regions are nothing but linear transformations of n-dimensional hypercubes. Note that the convenience of the ZF receiver comes from the fact that the destination lattice is $\mathbb{Z}^n$, which allows detection by means of a simple slicer.

We argue that it is possible to perform a linear transformation from any received lattice Λ onto other lattices in $\mathcal{M}$ which also lend themselves to another convenient detection method, namely, the Viterbi algorithm. Figure 6.1 depicts the set of all lattices, including the particular $\mathcal{L}_{\mathrm{R}}$ family. Any given lattice may be closer to one particular lattice in $\mathcal{L}_{\mathrm{R}}$ than to $\mathbb{Z}^n$, as there are infinitely many more in $\mathcal{L}_{\mathrm{R}}$. Again, notice that ZF will alwasy focus any received lattice onto $\mathbb{Z}^n$, regardless of the distance to it.

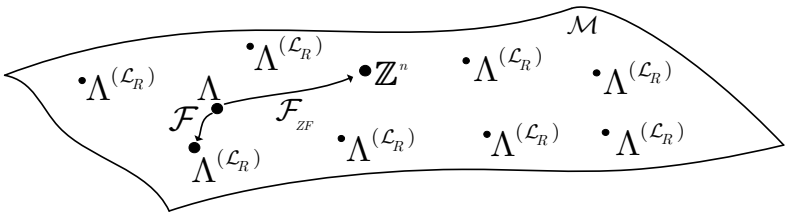


Figure 6.1: The set of lattices and the focusing operator. A received lattice Λ can be focused onto the nearest member of $\mathcal{L}_R$ or onto $\mathbb{Z}^n$.

When the distance between lattices is reduced, then the matching (or *coverage* [147]) between their decision regions is maximized, which minimises the distortion created by linearly transforming one lattice onto another one. If there is a member of $\mathcal{L}_{\mathrm{R}}$ near to Λ (i.e., very "similar" to Λ), then *i)* its MLD regions will closely match the ones of the original lattice and *ii)* the distortion involved in the focusing operation will be small. This concept opens doors to a new type of receiver comprising the blocks shown in Figure 6.2.

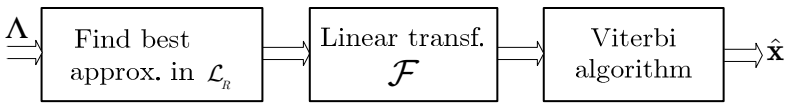


Figure 6.2: Detection on an approximated trellis representation.

6.3 — The $\mathcal{L}_R$ Family of Lattices

A lattice has a trellis if it can be written as the union of a *rectangular sublattice* Λ_R and translated versions of it. A rectangular lattice is a lattice whose orthogonality defect is one, i.e., all its generator vectors mutually are orthogonal. As noticed by Forney [214], in the language of group theory, such a lattice is described as

$$\Lambda = \Lambda_R + \left[\frac{\Lambda}{\Lambda_R}\right], \tag{6.1}$$

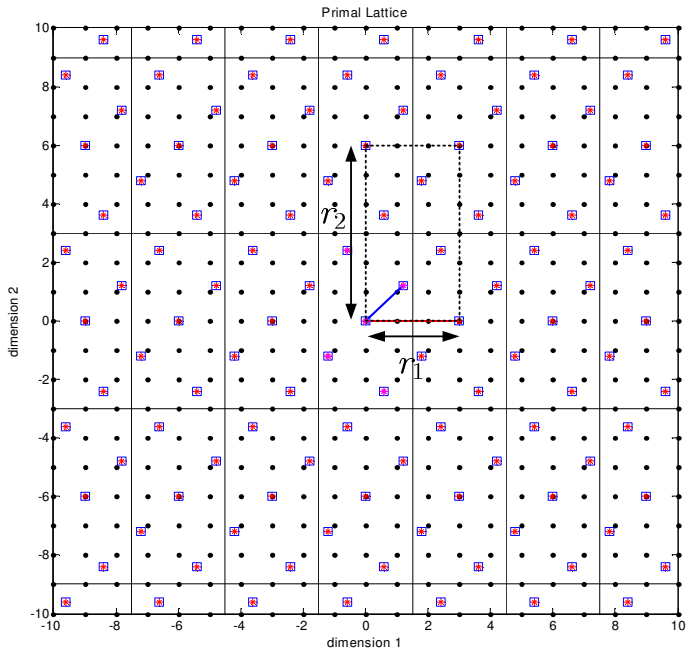
where $[\Lambda/\Lambda_R]$ is a *system of coset representatives* for the cosets of Λ_R in Λ or, equivalently, for the elements of the quotient group Λ/Λ_R (as it was introduced in section 6.1). As Λ_R is a rectangular lattice, by definition it can be expressed by a Cartesian product, i.e., $\Lambda_R = r_1\mathbb{Z}\times\cdots\times r_n\mathbb{Z}$. Geometrically, the fundamental region of the rectangular sublattice is an hyper-rectangle whose sides have lengths $r_1, r_2, \cdots, r_n$.

Figure 6.3 shows an example of a lattice in $\mathbb{Z}^2$ and its representation by a trellis. It is possible to observe the rectangular quotient group and its translated versions. The lattice is then the union of the cosets of Λ_R in Λ . For the case in Figure 6.3, the number of cosets (or the *index*) of Λ_R in Λ is $\Phi=|\Lambda/\Lambda_R|=5$. In general, the number of cosets is

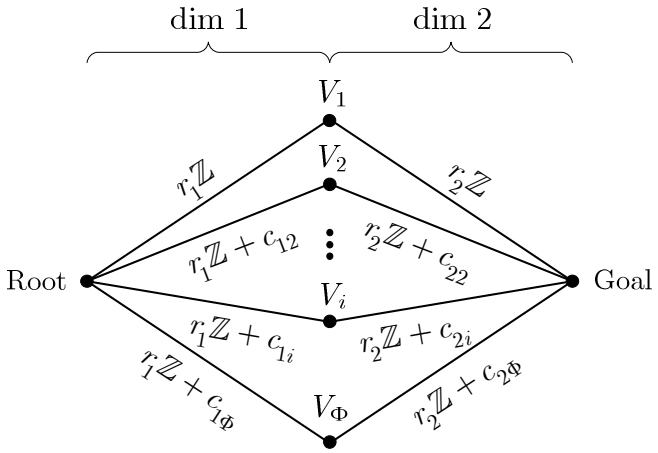
$$\Phi = \left|\frac{\Lambda}{\Lambda_R}\right| = \frac{\det(\Lambda_R)}{\det(\Lambda)}. \tag{6.2}$$

The trellis is characterised by an infinite number of paths connecting the root state to the goal state, however, the infinite number of paths only reflects the fact that a lattice has an infinite number of paths. The representation of the trellis can be made finite by describing a set of coset representatives. Other points in a particular coset are obtained by summing integer multiples of its coset representative, denoted in the trellis by $\mathbb{Z}$. Each point of the lattice that is a coset representative is defined by one of the paths connecting the root to the goal state. In Figure 6.3 (a) it is possible to observe an example of a partition of a lattice into its five cosets (i.e., $\Phi = 5$). Inside each rectangular region there is one representative of each one of the cosets. The trellis

representation of that lattice is shown in Figure 6.3 (b), where each coset representative has coordinates (c_{1i}, c_{2i}) , $i = 1, 2, \cdots, \Phi$. The finite set of possible coordinates that can exist at the i^{th} trellis step (i.e., the set of possible coordinates of coset representatives in dimension $i<n$) is called the *label group* in dimension i. Note that the origin of the lattice corresponds to the *zero path*.



(a) Rectangular sub-lattice in a lattice that has a trellis representation.



(b) Trellis of the 2D lattice.

Figure 6.3: A rectangular sub-lattice in a random lattice and the trellis representation of the lattice.

Using the origin as a representative of the rectangular sublattice Λ_R, the set constituted by the origin together with all the other points with coordinates (c_{1i}, c_{2i}), $i = 1,2,\cdots,\Phi$, that are inside the central rectangular region constitute then the *coset representatives* of the quotient group. The whole lattice can now be seen as a tiling of the space using that fundamental region, i.e., tiling with the hyper-rectangles of volume $r_1 \times r_2 \times \cdots \times r_n$. This is also illustrated for the hexagonal lattice A_2 in Figure 6.4.

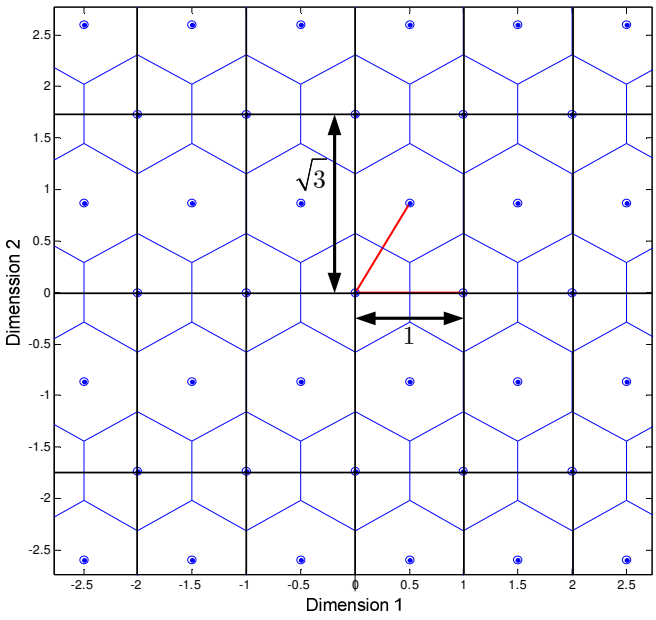


Figure 6.4: The rectangular quotient group of the A_2 lattice, exhibiting two cosets.

Figure 6.5 and Figure 6.6 respectively show possible trellises for the Schläfli lattice, D_4, and for the Gosset lattice, E_8 [20], [210]. Notice that some lattices may have several different trellis representations if they possess several different orthogonal sublattices (below each trellis the label groups in each dimension are indicated).

The n-dimensional orthogonal sublattice has its basis vectors along one-dimensional subspaces W_i, i=1,...,n. From these we can define the sequence of spaces $\{\mathbf{0}\} \subset V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ and each W_i, is the 1D orthogonal complement of V_{i-1} to V_i. The projections onto V_i and W_i are respectively denoted by P_i and P_{W_i}. One must also define the intersection lattices, $\Lambda_i = \Lambda \cap V_i$, and also the one-dimensional lattices,

$\Lambda_{W_i} = \Lambda \cap W_i$. Using these definitions, the state space of a trellis of a lattice in the coordinate system $\{W_i\}_{i=1}^{n}$ is defined by the quotient group $P_i(\Lambda) / \Lambda_i$ and the label group for the trellis branches is given by $P_{W_i}(\Lambda) / \Lambda_{W_i}$. This construction is best described in [219], [220], [219], and more recently in [221]. However, applying this method to non-integer lattices (or those without an unusually small determinant) faces numerical challenges. Indeed, the cited works deal with lattices whose HNF is simple to compute and therefore obtaining the projection lattices becomes a simple task. That is not the case for random Gaussian lattices and finding a suitable trellis construction method is left as an open problem in this dissertation.

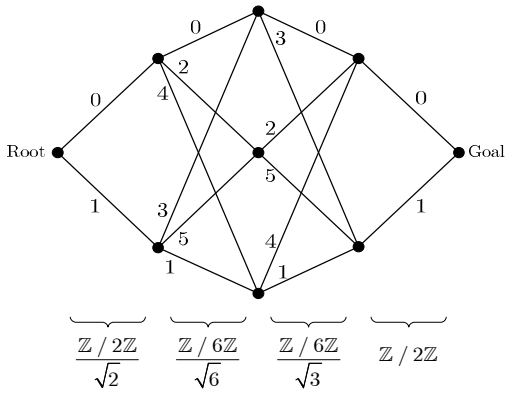


Figure 6.5: One of the possible trellises of the Schläfli lattice, D_4 (with 6 paths).

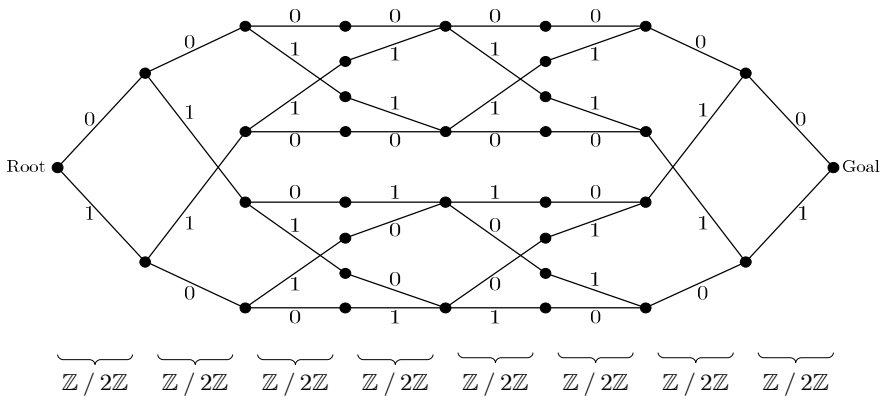


Figure 6.6: One of the possible trellises of the Gosset lattice, E_8 (with 16 paths).

6.4 – Lattices with Orthogonal Sublattices

In order to be able to create lattices that are members of the $\mathcal{L}_R$ family, one first needs to understand what properties a generator matrix must hold. The second step will be devising an algorithm that creates a lattice $\Lambda \in \mathcal{L}_R$, which is geometrically "similar" to a certain given Gaussian lattice.

6.4.1 – The Quasi Orthogonal Sublattice Problem

A lattice can only be written in the form (6.1) if and only if it contains a rectangular sublattice. Given a lattice, to find a rectangular sublattice within it is believed to be itself an NP-hard problem, even if it is known that at least one such sublattice exists. The problem is NP-hard even if the search is relaxed to finding a quasi-orthogonal sublattice. Micciancio calls this problem the *quasi orthogonal set problem* in [222] (ch.7), and one may also appropriately call this the *quasi orthogonal sublattice problem* (QOSP). This problem has received virtually no attention in the literature, apparently owing to a lack of applications.

In addition to the problem of discovering a rectangular sublattice we add an additional constraint: one wants to find the rectangular sublattice that minimises the index number of the quotient group in order to minimise the number of trellis paths. Instead of looking for an orthogonal sublattice (which may not even exist), a fruitful approach is to look for a near lattice that well approximates the first one, while having an orthogonal sublattice. For this purpose one needs to recall the definition of a $(\mathbf{H}, \varepsilon)$-*neighbourhood* of a lattice, given in Chapter 5.

A Frobenius distance between the two matrices provides a continuous metric that measures how close two lattices are from each other:

$$\left\|\mathbf{H}-\mathbf{H}'\right\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |\, h_{ij} - h'_{ij} \,|^2} = \mathrm{Trace}\Big((\mathbf{H}-\mathbf{H}')^T(\mathbf{H}-\mathbf{H}')\Big). \tag{6.3}$$

Expression (5.6) is a sufficient but not necessary condition for two lattices to be similar, or indeed the *same*. Notice that, as seen in Chapter 2, two lattices can be the

same if their generator matrices are related by right-side multiplication by a unimodular matrix. Moreover, any basis of a rational lattice can be brought to a unique canonical form using the Hermite Normal Form (HNF), as mentioned in Chapter 5. However, a lattice can also be geometrically equivalent up to orthogonal rotations (and scaling). If one takes a certain lattice and scale it by a real number, it is not difficult to accept that the lattice is, "in a certain way", the *same*. The same argument holds if one simply rotates the lattice around any set of axes or concatenates several of these scaling and rotation operations; the resulting lattice is also the *same.* A complex lattice generated by a basis $\mathbf{H}$ is equivalent to a lattice defined by a matrix $\widehat{\mathbf{H}}$ if and only if

$$\widehat{\mathbf{H}} = \left(\frac{\mathrm{vol}(\widehat{\mathbf{H}})}{\mathrm{vol}(\mathbf{H})}\right)^{\frac{1}{d}} \cdot \mathbf{U} \cdot \mathbf{H} \cdot \mathbf{M}\,, \tag{6.4}$$

where $\mathbf{U}$ and $\mathbf{M}$ are respectively a unitary (or orthogonal for real lattices) and a unimodular matrix and the term involving the volumes is the appropriate scaling factor.

This geometric equivalence is chiefly overlooked in the lattice literature, as Agrell pointed out in [116]. To the best of our knowledge, the *lattice distinguishing problem* (LDP), i.e., deciding if two given lattices are the same still remains an open problem. Some work has been conducted on a limited version of this general problem: the authors of [223] and [224] dealt with the LDP for lattices isomorphic to $\mathbb{Z}^n$ given their Gram matrix but more work in this field is necessary. Expression (6.4) defines an *equivalence relation* (e.g., [206]) between pairs of bases.

It is not difficult to see that the LDP is closely related the problem of finding a lattice in $\mathcal{L}_R$. Consider a lattice with basis

$$\mathbf{H} = \begin{bmatrix} 6 & 3.6 \\ 0 & 2 \end{bmatrix}. \tag{6.5}$$

This lattice has a rectangular sublattice with $r_1 = 6$ and $r_2 = 10$, as can be seen in Figure 6.7 (lattice with "*" inside squares). Now, consider the basis

$$\tilde{\mathbf{H}} = \mathbf{Q}\mathbf{H} = \begin{bmatrix} 5.98 & 3.41 \\ 0.52 & 2.30 \end{bmatrix}, \tag{6.6}$$

obtained from $\mathbf{H}$ with a rotation matrix $\mathbf{Q}$ that rotates the generators of $\mathbf{H}$ by 5 degrees anticlockwise. The resulting lattice is also plotted in Figure 6.7 (lattice with simple "*"). Consider now the reverse case, where one starts with basis $\tilde{\mathbf{H}}$. a slight rotation of the lattice would allow a simple coset partition. However, there is no algebraic method to discover that. If, in addition to the rotation, the two bases are also related by a unimodular transformation, then the problem is even harder.

Finding a lattice that is a member of $\mathcal{L}_{\mathrm{R}}$ and which simultaneously lies in a certain $(\mathbf{H}, \varepsilon)$ -neighbourhood of Λ is a problem without an analytical solution unless the hierarchy of the complexity classes described in section 1.3.1 collapses; consequently, one resorts to an algorithmic approach, which will be presented in the next sub-section.

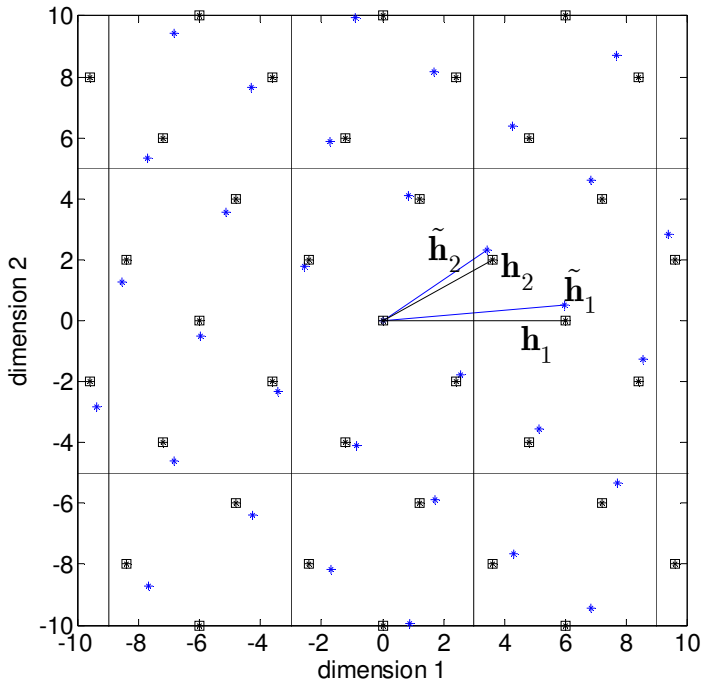


Figure 6.7: A lattice given by $(\mathbf{h}_1, \mathbf{h}_2)$ with a rectangular sublattice (with its points "*" inside squares) and a near lattice generated by $(\tilde{\mathbf{h}}_1, \tilde{\mathbf{h}}_2)$, obtained from $(\mathbf{h}_1, \mathbf{h}_2)$ rotated by 5 degrees anticlockwise (depicted by "*").

The seminal work by Paz and Schnorr [136] (later generalised by Trolin [137]) proved that there is always a lattice with one-cycle in any neighbourhood of any integer lattice. Moreover, those lattices have a trellis structure because a cyclic lattice always has $\mathbb{Z}^n$ as a sublattice, and $\mathbb{Z}^n$ is just a particular case of a rectangular sublattice. Unfortunately, the two methods provided by [136] and [137] are only valid for integer lattices and scaling a rational $\mathbf{H}$ to yield integer entries makes the application of both methods numerically impracticable.

Furthermore, some lattices are known to have the cubic sublattice $\mathbb{Z}^n$ embedded in them. The work by Oggier and Viterbo used methods from algebraic number theory to construct such lattices [77], [79]. However, given the LDP, deciding if one of these lattices can well approximate any random lattice seems an intractable problem.

6.4.2 — Properties of the Generator Matrix

Let us consider a random rational lattice defined by a rational $\mathbf{H}$ with entries $h_{ij} = n_{ij} / d_{ij}$ and whose inverse is the rational matrix $\mathbf{W}=\mathbf{H}^{-1}$ with entries p_{ij} / q_{ij}. The existence of a rectangular sublattice Λ_R imposes the existence of lattice points $y = [y_1, y_2, \cdots y_n]^T$ whose coordinates are a multiple of the length of the respective dimension of the hyper-rectangle, that is, each coordinate y_i must be of the form kr_i, for $k \in \mathbb{Z}$ and $i = 1,2,\cdots,n$. Now, because $\mathbf{x} = \mathbf{H}^{-1}\mathbf{y}$ (without noise), this imposes

$$\begin{bmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \frac{p_{11}}{q_{11}} & \frac{p_{12}}{q_{12}} & \cdots & \frac{p_{1n}}{q_{1n}} \\ \frac{p_{21}}{q_{21}} & \frac{p_{22}}{q_{22}} & \cdots & \frac{p_{2n}}{q_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{p_{n1}}{q_{n1}} & \frac{p_{n2}}{q_{n2}} & \cdots & \frac{p_{nn}}{q_{nn}} \end{bmatrix} \cdot \begin{bmatrix} kr_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{p_{11}}{q_{11}} kr_1 \\ \frac{p_{21}}{q_{21}} kr_1 \\ \vdots \\ \frac{p_{n1}}{q_{n1}} kr_1 \end{bmatrix} \tag{6.7}$$

for $k \in \mathbb{Z}$. By definition of a lattice , $x_1 \in \mathbb{Z}$, $x_2 \in \mathbb{Z}$, $\cdots x_n \in \mathbb{Z}$, and therefore one has

$$\begin{cases} \frac{p_{11}}{q_{11}} k r_1 \in \mathbb{Z} \\ \frac{p_{21}}{q_{21}} k r_1 \in \mathbb{Z} \\ \quad \vdots \\ \frac{p_{n1}}{q_{n1}} k r_1 \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} \frac{r_1}{q_{11}} \in \mathbb{Z} \\ \frac{r_1}{q_{21}} \in \mathbb{Z} \\ \quad \vdots \\ \frac{r_1}{q_{n1}} \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} q_{11} \Big| r_1 \\ q_{21} \Big| r_1 \\ \quad \vdots \\ q_{n1} \Big| r_1 \end{cases} \tag{6.8}$$

In general, $\frac{p_{i1}}{q_{i1}} k r_1 \in \mathbb{Z} \Rightarrow \frac{r_1}{q_{i1}} \in \mathbb{Z}$ and thus $q_{i1} \Big| r_1$, where $q_{i1} \Big| r$ denotes that q_{i1} divides r . Hence,

$$r_1 = \mathrm{lcm}\left(q_{11}, q_{21}, \cdots, q_{n1}\right). \tag{6.9}$$

where lcm stands for *lowest common multiple*.

Applying the same reasoning to each dimension one concludes the following rule for the lengths of each side of the fundamental region of the rectangular sublattice

$$r_i = \mathrm{lcm}\left(q_{1i}, q_{2i}, \cdots, q_{ni}\right). \tag{6.10}$$

Finally, because (6.10) is associated with the rows of $\mathbf{H}^{-1}$ in (6.7), and remembering that the dual matrix is $\mathbf{H}^{(D)} = (\mathbf{H}^{-1})^T$, it is equivalent to say that (6.10) sets a property for the (column) generator vectors of the generator matrix of the dual lattice. In conclusion, the sublattice Λ_R of $\Lambda \in \mathcal{L}_R$ in the original system of coordinates is completely specified by the lowest common multiple of the denominators q_{ij} of its dual matrix, i.e.,

$$r_i = \mathrm{lcm}\left(q_{i1}, q_{i2}, \cdots, q_{in}\right), \; i = 1,2,\ldots n \,. \tag{6.11}$$

Later, in section 6.4.4, an algorithm will be presented to generate lattices in $\mathcal{L}_R$ by imposing that all the denominators q_{ij} are identical within a particular row i.

6.4.3 — Geometrical Interpretation: Distortion vs Number of Cosets

The number of cosets in a quotient group (i.e., the index of the sublattice Λ_R) is

$$\Phi = \left|\frac{\tilde{\Lambda}}{\Lambda_R}\right| = \frac{\mathrm{Vol}\left(\Lambda_R\right)}{\mathrm{Vol}\left(\tilde{\Lambda}\right)} = \frac{\prod_{i=1}^{n} r_i}{\det\left(\tilde{\mathbf{H}}\right)} = \prod_{i=1}^{n} r_i \cdot \det\left(\tilde{\mathbf{H}}^{(D)}\right). \tag{6.12}$$

In order to calculate $\det(\tilde{\mathbf{H}}^{(D)})$ one may notice that the approximated dual lattice in (6.17) is uniquely defined by two matrices: one is $\mathbf{P}$, comprising the denominators, and the other is $\mathbf{R}$, constituted by the numerators of $\tilde{\mathbf{H}}^{(D)}$, and both matrixes are u.t.:

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ 0 & p_{22} & \cdots & p_{21} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_{nn} \end{bmatrix} \quad , \quad \mathbf{R} = \begin{bmatrix} r_1 & r_1 & \cdots & r_1 \\ 0 & r_2 & \cdots & r_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & q_n \end{bmatrix}. \tag{6.13}$$

Note that the non-zero elements of $\mathbf{R}$ in each row are forced to be equal. Consequently, the determinant of $\tilde{\mathbf{H}}_D$ can be obtained as

$$\det\left(\tilde{\mathbf{H}}_D\right) = \prod_{i=1}^{n} \frac{p_{ii}}{r_i} = \underbrace{\prod_{i=1}^{n} p_{ii}}_{\substack{\text{product diagonal} \\ \text{numerators}}} \cdot \underbrace{\prod_{i=1}^{n} \frac{1}{r_i}}_{\substack{\text{volume of} \\ \text{quantization grid}}} \quad , \tag{6.14}$$

and (6.12) becomes

$$\Phi = \left|\frac{\tilde{\Lambda}}{\Lambda_R}\right| = \prod_{i=1}^{n} r_i \cdot \prod_{i=1}^{n} p_i \cdot \prod_{i=1}^{n} \frac{1}{r_i} = \prod_{i=1}^{n} p_i \,. \tag{6.15}$$

The number of cosets is thus solely determined by the diagonal of **P**. It is possible to obtain a geometrical insight into the problem by expressing the number of cosets as

$$\begin{aligned} \Phi &= \left|\frac{\tilde{\Lambda}}{\Lambda_R}\right| = \frac{\mathrm{Vol}\left(\Lambda_R\right)}{\mathrm{Vol}\left(\tilde{\Lambda}\right)} = \mathrm{Vol}\left(\Lambda_R\right)\mathrm{Vol}\left(\tilde{\Lambda}_D\right) \\ &= \prod_{i=1}^{n} r_i \cdot \mathrm{Vol}\left(\tilde{\Lambda}_D\right) = \mathrm{Vol}\left(\tilde{\Lambda}_D\right) \Big/ \frac{1}{\prod_{i=1}^{n} r_i} = \frac{\mathrm{Vol}\left(\tilde{\Lambda}_D\right)}{\mathrm{Vol}(\varepsilon_q)}. \end{aligned} \tag{6.16}$$

In section 6.4.4 an algorithm will be presented that forces the coordinates of the basis of $\tilde{\Lambda}^{(D}$ in dimension i to *all* be expressed with the same denominator r_i. Hence, the denominator $\left(\prod_{i=1}^{n} r_i\right)^{-1}$ in (6.16) corresponds to the volume of what can be interpreted as a "quantisation grid", with quantisation steps r_i^{-1} in dimension i.

The following dilemma can be identified: on the one hand, a good approximation of a dual lattice requires a large r_i in each dimension, i.e., a small "quantisation step". On

the other hand, because each entry in $\tilde{\mathbf{H}}^{(D)}$ is in the rational form p_{ij} / r_i , a larger r_i implies a larger p_{ij} ; in particular, the numerators in the diagonal, p_{ii} , would also become larger and, from (6.15), the number of cosets Φ grows, contrary to what is desired. This is illustrated in Figure 6.8 where both the volume of the dual lattice and the volume of the quantization grid are shown. Note that, according to (6.16), the ratio of these two volumes gives Φ , which one wants to minimise.

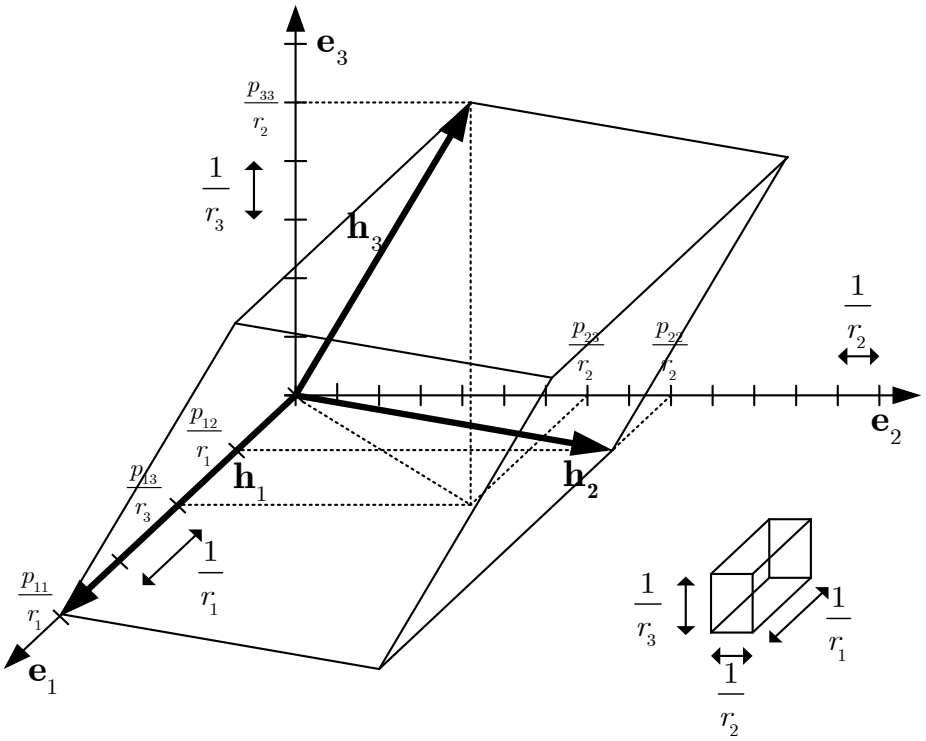


Figure 6.8: Approximation versus number of cosets: the dilemma of the approximation in the dual lattice (example in a 3D space).

In order to reduce the number of paths in the trellis of a lattice in $\mathcal{L}_R$, one wants to keep low value entries in diag($\mathbf{P}$) , while at the same time, a good approximation that minimises $\left\|\mathbf{H}^{(D)} - \tilde{\mathbf{H}}^{(D)}\right\|_F$, implies having large r_i values (as these ratios are fixed, this constitutes another constraint for the problem).

6.4.4 — Lattice Construction Algorithm

In view of (6.11), and remembering that the lattice equivalence problem is intractable, instead of searching for a lattice in the neighbourhood by means of orthogonal or unimodular transformations, the problem will be reduced to finding a close (in the Frobenius sense) dual generator matrix. For that purpose, one starts by applying a QR decomposition to the dual matrix, reducing it to the upper triangular (u.t.) form via a rigid rotation of the lattice, $\mathbf{Q}$. To make the elements in this matrix shorter, we *i)* LLL-reduce this rotated dual lattice and then *ii)* find rational approximations for the matrix elements via a greedy algorithm. (Notice that the Diophantine approximation problem is itself a NP-hard problem, solvable by mapping it onto another CVP [110]). Algorithm 3.1, presented bellow, finds an approximated (or "synthetic") dual lattice of the form

$$\tilde{\mathbf{H}}^{(D)} = \left(\mathbf{h}_1^{(D)}\ \mathbf{h}_2^{(D)} \cdots \mathbf{h}_n^{(D)}\right) = \begin{pmatrix} \frac{p_{11}}{r_1} & \frac{p_{12}}{r_1} & \cdots & \frac{p_{1n}}{r_1} \\ 0 & \frac{p_{22}}{r_2} & \cdots & \frac{p_{2n}}{r_2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \frac{p_{nn}}{r_n} \end{pmatrix}. \tag{6.17}$$

The core of Algorithm 3.1 is carried out on the dual matrix $\mathbf{H}^{(D)}$. The algorithm starts by shortening the generator vectors of $\mathbf{H}^{(D)}$ and then sorts them in ascendant order of their norm from the leftmost column to the rightmost one. This procedure minimises p_{11} and therefore constitutes a first step towards minimising Φ, from (6.15). The algorithm then enters a search mode where in each step the largest numerator p_{ii} is found and its accuracy relaxed so that p_{ii} may diminish. Then, all the remaining off-diagonal elements in that row are written with the denominator that has just been found, so that $r_i = q_{ii}$, as seen in (6.17). The rational approximation of the diagonal elements is relaxed by means of a continuous fraction algorithm.

Figure 6.9 and Figure 6.10 show two examples of how the number of cosets evolves as the error tolerance δ increases. At the same time, it is also possible to

see the corresponding increase of the Frobenius distance between the synthetic dual lattice and the original dual lattice, $\left\|\mathbf{H}^{(D)} - \tilde{\mathbf{H}}^{(D)}\right\|_F$ (this metric is shown in both figures as a percentage of $\left\|\mathbf{H}^{(D)}\right\|_F$). Notice that this is the distance between the dual lattices and *not* the distance between the primal lattices (as matrix inversion changes the Frobenius norm).

ALGORITHM 6.1: SYNTHESIS OF A LATTICE IN $\mathcal{L}_R$

Input: Generator $\mathbf{H}$, Admissible numb. of paths Γ.

Output: Approximation $\tilde{\mathbf{H}} \in \mathcal{L}_R$; number of cosets $|C|$.

1: $\mathbf{H}_{\text{red}}^{(D)}, \mathbf{M} \leftarrow \text{LLL}\{(\mathbf{H}^{-1})^T\}$, $\mathbf{M}$ is unimodular

2: $\mathbf{U}, \widehat{\mathbf{H}}_{\text{red}}^{(D)}, \mathbf{J} \leftarrow QR\left(\text{sort}(\mathbf{H}_{\text{red}}^{(D)})\right)$; $\mathbf{J}$ is a permutation, $\widehat{\mathbf{H}}_{\text{red}}^{(D)}$ is upper triangular and $\mathbf{U}$ is orthogonal.

3: $\mathbf{P}, \mathbf{Q} \leftarrow \mathbf{H}^{(D)}$, such that $h_{ij}^{(D)} = p_{ij} \,/\, q_{ij}$

4: Calculate Φ from (6.15)

5: Do until $\Phi < \Gamma$

6: Find $l = \arg\max_i \{p_{ii}\}$ and approximate $p_{ll} \,/\, q_{ll}$ by another rational having smaller p_{ll} and smaller q_{ll}.

7: $r_i \leftarrow q_{ii}$

8: Obtain $\tilde{\mathbf{H}}_{\text{red}}^{(D)}$: for row l, write the off-diagonal $p_{lj} \,/\, q_{lj}$ using a common denominator r_i and with maximum error δ.

9: $\mathbf{P}, \mathbf{R} \leftarrow \tilde{\mathbf{H}}_{\text{red}}^{(D)}$; as in (6.13)

10: $\left|C\right| = \prod_{i=1}^{n} p_i$, as in (6.15)

11: increment δ

12: end loop

13: $\tilde{\mathbf{H}} = \mathbf{U}^T \left((\tilde{\mathbf{H}}_{\text{red}}^{(D)} \cdot \mathbf{J}^{-1})^{-1}\right)^T \mathbf{M}^{-1}$

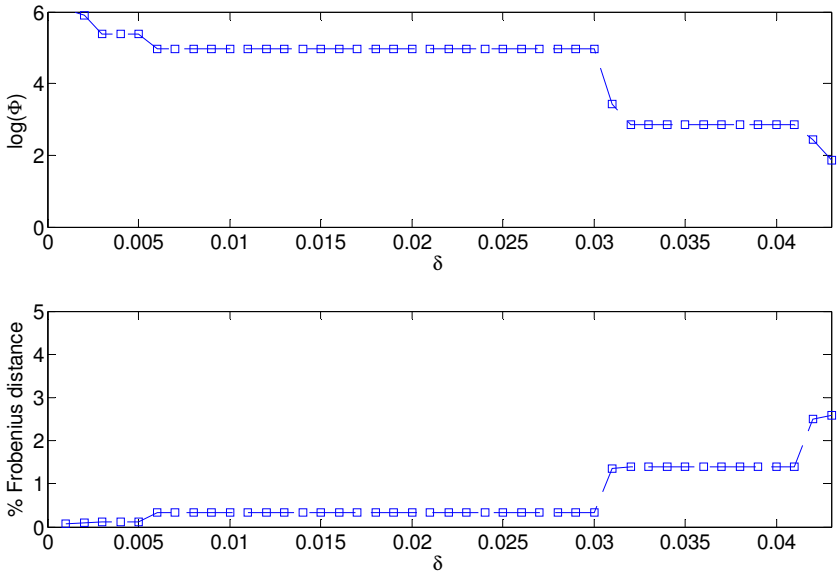


Figure 6.9: Evolution of the number of cosets and Frobenius distance in Algorithm 3.1 for a n=4 dimensional random lattice as the error tolerance increases.

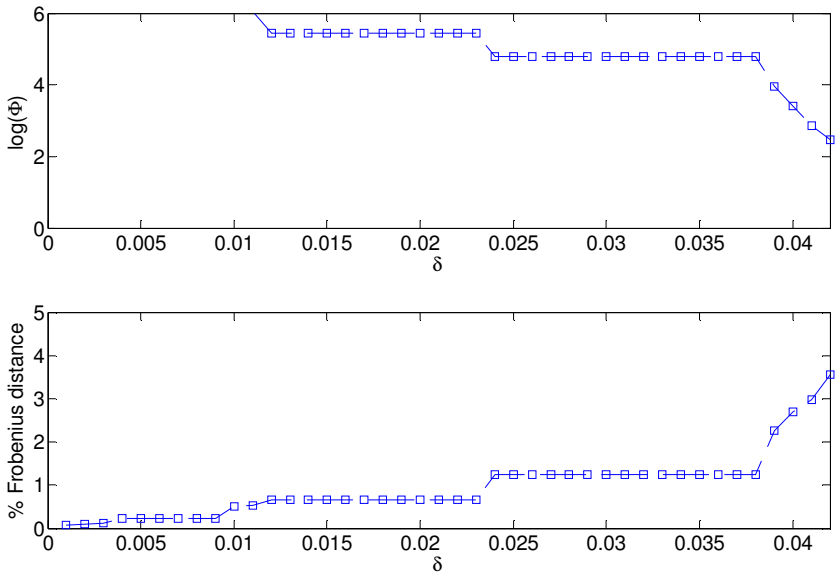


Figure 6.10: Evolution of the number of cosets and Frobenius distance in Algorithm 3.1 for a n=8 dimensional random lattice as the error tolerance increases.

In Figure 6.9 the algorithm was set to run in n=4 dimensions, with $\Gamma = 100$; it terminated after 43 iterations, returning a lattice in $\mathcal{L}_{\mathrm{R}}$ with $\Phi = 75$ cosets. Figure 6.10

shows an example for n=8, with $\Gamma = 500$; the algorithm found a lattice with Φ=324 after 144 iterations.

The complexity of Algorithm 1 is dominated by the LLL reduction, $\mathcal{O}(n^4)$. In addition, the QR decomposition is $\mathcal{O}(n^3)$, sorting is $\mathcal{O}(n\log n)$ [225] (sec. 6.5), and the iterations for rational approximation is dominated by a continued fractions algorithm, having $\mathcal{O}(n^3)$ [226] . Sphere decoding is well known to have a random number of branch expansions during the exploration of the tree (unless fixed complexity sphere decoding is used [190]). That number varies each time a received vector is decoded, and is highly dependent upon the noise power. We note that, while in the proposed detector the number of cosets is also a random variable, it only affects the pre-processing stage. Then, the complexity remains constant over the coherence time of that lattice instance.

6.5 — Number of Cosets

As the decoding complexity is strictly associated with the number of cosets, it is necessary to investigate the number of cosets, Φ , in the lattices output by Algorithm 6.1. Note that Φ depends only on the channel realisation and not on the modulation that is chosen. Hence, it is possible to study the number of cosets *per se*.

In Algorithm 6.1 there is a trade-off between the maximum admissible number of cosets, Γ , the increment δ in the error tolerated in each element of the channel matrix, and the number of iterations required to find a lattice that satisfies the limit. A smaller error increment increases the probability of finding a suitable lattice (with $\Phi < \Gamma$) that is closer to the original one than if a lattice is found latter on, having a much larger value of δ. It was found that there is a probability that Algorithm 6.1 has to perform many iterations to find a suitable lattice. Consequently, a limit was imposed on the number of iterations. It was found heuristically that, regardless of the number of dimensions, a good option was to limit the number of iterations to 1,000 while using an error tolerance increment $\delta = 0.001$. In the last possible iteration, this choice of parameters leads to a maximum error tolerance of 1.0 in the rational approximation of each element in the diagonal of $\tilde{\mathbf{H}}$ (obtained via a continued fraction method).

However, owing to step 8 in Algorithm 6.1 , the errors in the off-diagonal elements may be larger.

The procedure used to search for the value of Γ to be set in the algorithm was to find the lowest value that would still lead to a quasi-optimum performance (the results of which will be presented in the next section) or, when that becomes too difficult to achieve (namely, in the cases of 8 and 12 dimensions), find the value of Γ that achieves the best possible performance.

The average number of cosets in the lattice returned by the algorithm is always $E\{\Phi\} < \Gamma$, however, there are particular instances when a lattice cannot be found with a number of cosets $\Phi < \Gamma$. Those instances are counted in the rightmost bin in the histograms shown in Figures 6.11 to 6.16, and are indicated by "*" above the bin. The visible domain of each probability distribution function (pdf) depicted in this section is chosen for "*"to represent not more than 1 per cent of the lattices. Moreover, the histograms are presented with an area normalised to 1, so that they can be a good approximation to pdfs. The total number of lattices taken into account corresponds to the sum of all the instances considered to obtain each of the points in the SER curves (which will be presented in section 6.6). When that information is meaningful, the figures also include a graphical representation of the standard deviation as a bar on top of the pdf and centred at the average. Because the pdf are wide, the standard deviation bar sometimes extends beyond the domain that is plotted, and thus the bar is omitted in these cases.

As expected, as the dimensionality goes up, the average number of cosets, $E\{\Phi\}$, required for quasi-optimal detection, also grows, however it is found that $E\{\Phi\}$ is still affordable up to 8 dimensions (4×4), which includes the most important scenarios in MIMO.

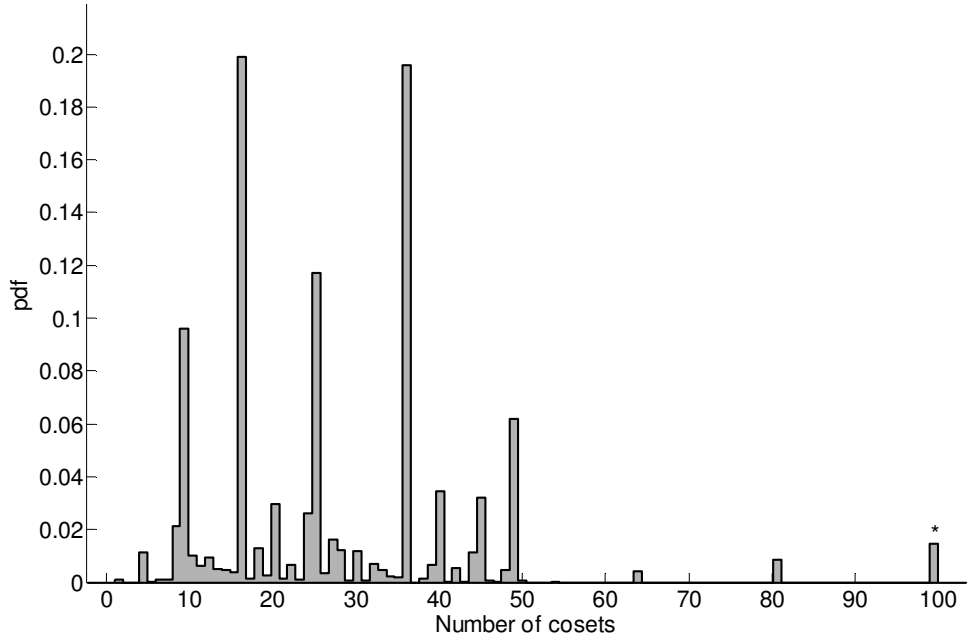


Figure 6.11: Probability density function of the number of cosets in n=4 real dimensions (2×2 configurations), limiting to Γ=50.

One surprising result is that the pdfs showing the number of cosets present in the various dimension sizes analysed are far from being uniform. Indeed, for all the dimension sizes investigated, and regardless of the limit Γ, the number of cosets tends to cluster around some particular numbers and the resulting probability density functions (pdfs) are "almost discrete" and "almost periodic", though they cannot strictly be considered as such. This fact is difficult to explain and can only be justified by the existence of an underlying number theoretic property governing the possible number of coset groups in n dimensions, which is a mathematical problem beyond the scope of this engineering approach. This property can be observed throughout the entire domain of the various pdfs. For example, in Figure 6.11 the maximum number of cosets tolerated was set to $\Gamma = 50$, but the same effect is visible if one sets $\Gamma = 100$, allowing us to observe a larger domain for Φ, as shown in Figure 6.12. Moreover, the same behaviour is found in all the other dimensions analysed: 6, 8 and 12 dimensions (i.e., 3×3, 4×4 and 6×6 antenna arrangements), as shown in Figures 6.9 to 6.14.

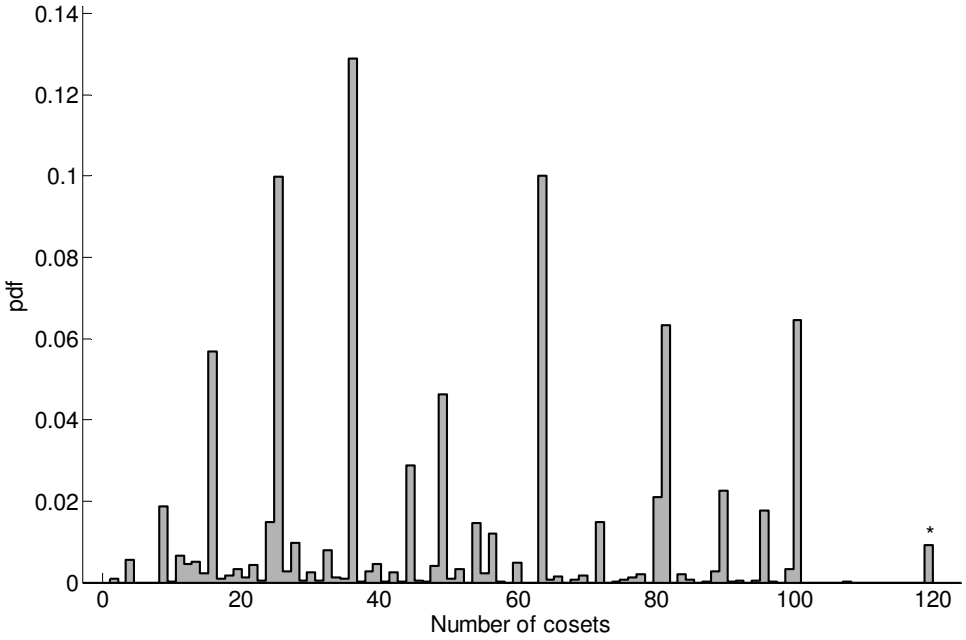


Figure 6.12: Probability density function of the number of cosets in n=4 real dimensions (2×2 configurations), limiting to Γ=100.

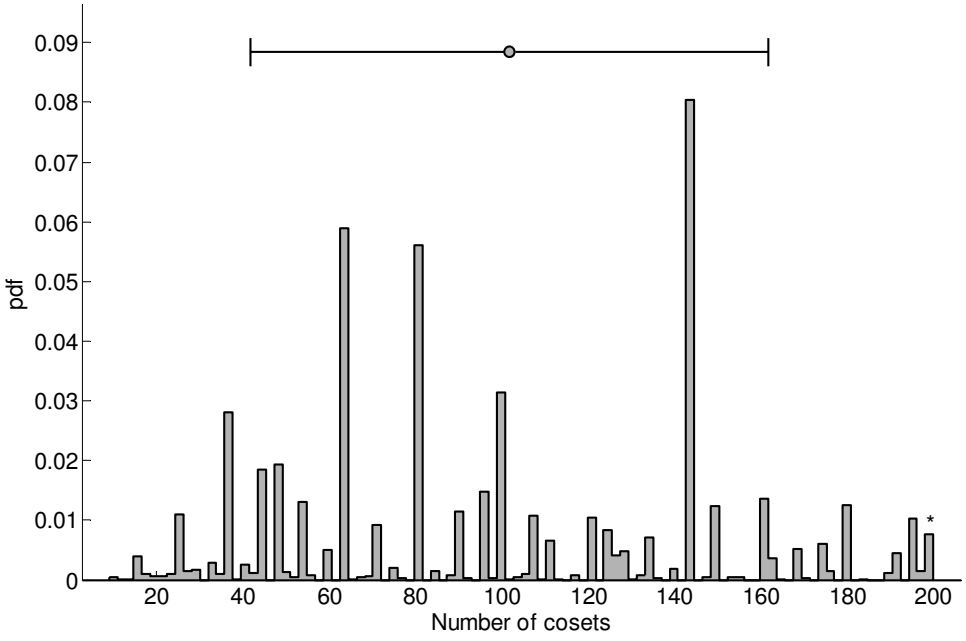


Figure 6.13: Probability density function of the number of cosets in n=6 real dimensions (3×3 configurations), limiting to Γ=200.

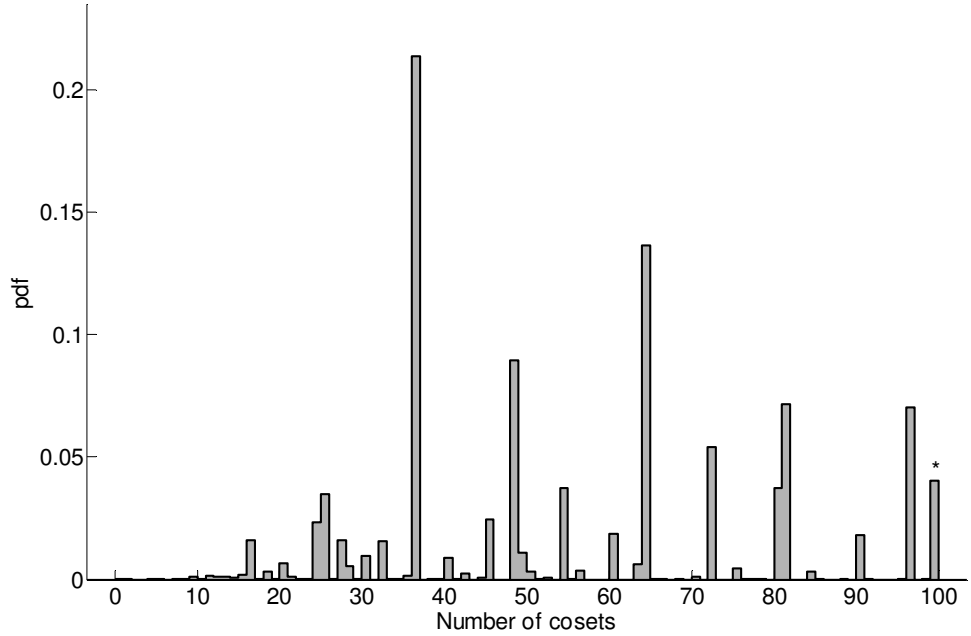


Figure 6.14: Probability density function of the number of cosets in n=8 real dimensions (4×4 configurations), limiting to Γ=100.

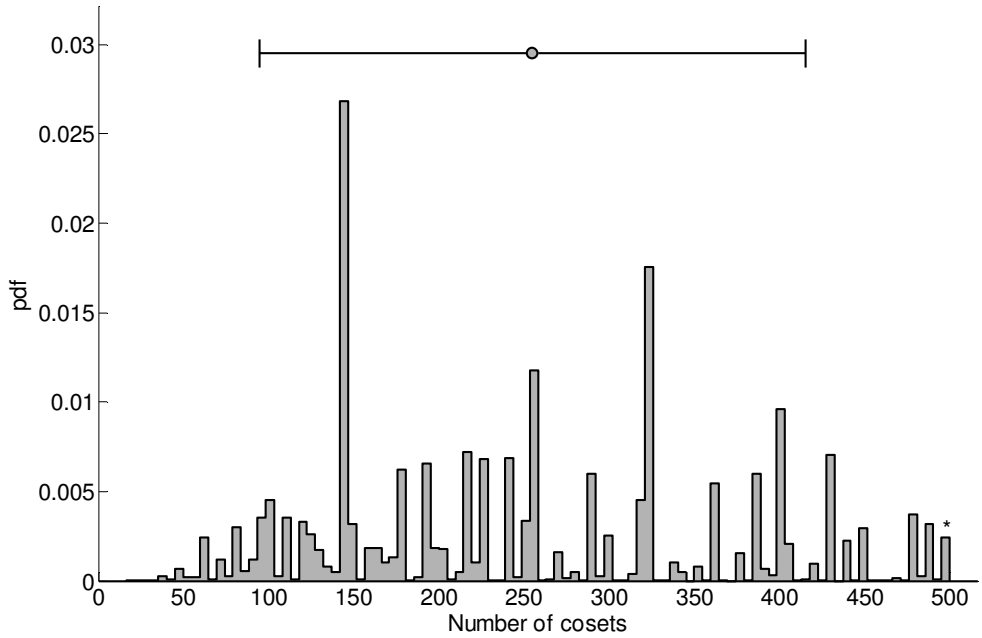


Figure 6.15: Probability density function of the number of cosets in n=8 real dimensions (4×4 configurations), limiting to Γ=500.

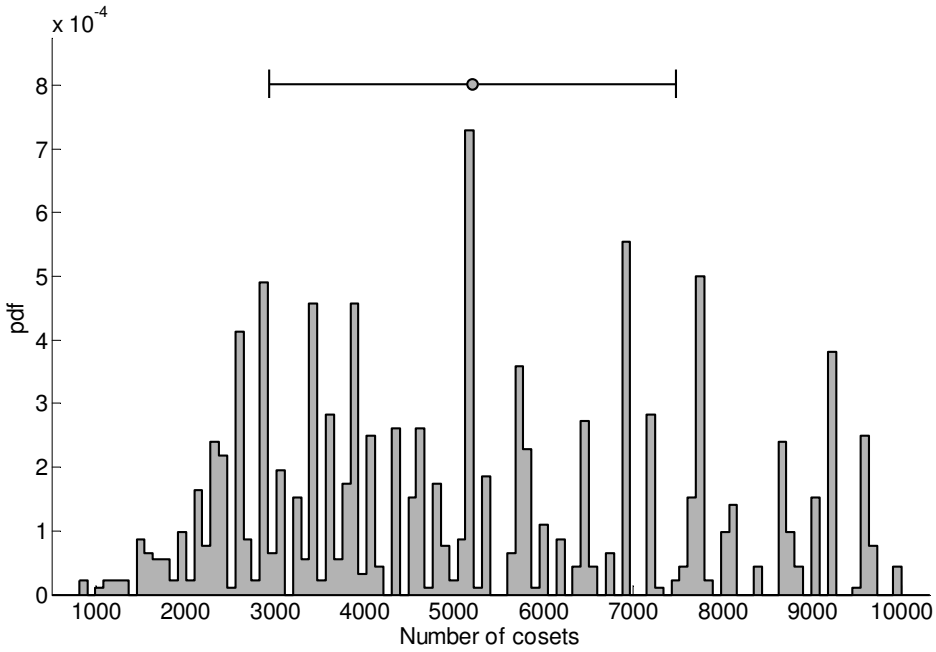


Figure 6.16: Probability density function of the number of cosets in n=12 real dimensions (6×6 configurations) , limiting to Γ=10,000.

Despite typical configurations in wireless MIMO having no more than 4 antennas, it is known that the standards such as LTE-A or 802.11ac are defined up to eight layers. Therefore, the case in 12 dimensions (6×6 antennas) was also investigated (Figure 6.16) so that a better assessment of how the number of cosets grows with the number of dimensions could be obtained.

6.6 — Performance Comparison

The Algorithm 6.1 outputs the approximated lattice $\tilde{\Lambda}$, which, by construction, should have Voronoi regions similar to the ones of the original Λ. Using the concept introduced in Section 6.2, the focusing linear transformation is

$$\mathcal{F}(\mathbf{H}, \tilde{\mathbf{H}}) = \tilde{\mathbf{H}} \cdot \mathbf{H}^{-1}, \tag{6.18}$$

with $\mathcal{F}$ close to the identity matrix, i.e., $\left\| \mathcal{F} - \mathbf{I} \right\|_F < \varepsilon$. By allowing an increasing number of cosets, ε can be brought close to zero.

This section presents the detection performance by Algorithm 3.1, after applying the linear transformation $\mathcal{F}(\mathbf{H}, \tilde{\mathbf{H}})$, given in (6.18). The exact performance is obtained using

a sphere decoder of the type previously described in Chapter 3. In doing this it is possible to assess the performance of applying the Viterbi algorithm to the trellis associated with the synthetic lattices.

For a proper comparison with other detection techniques, simulations have been run in a Rayleigh flat fading channel and, as in Chapter 3, the results are compared with the following detection techniques: ZF and MMSE, OSIC (i.e., the typical V-BLAST), and LLL-based lattice reduction pre-processing followed either by ZF or by OSIC. In order to assess the power penalty in respect to MLD, its performance is also shown, obtained with a SD of the type described in Chapter 3. Note that the reason for the use of the SD here is to obtain the optimal performance of the SM schemes considered, and for that reason more sophisticated (and with lower complexity) SD algorithms are not necessary. The results will now be presented for the typical M-QAM alphabets and are grouped according to the number of dimensions.

6.6.1 — 2×2 Antennas

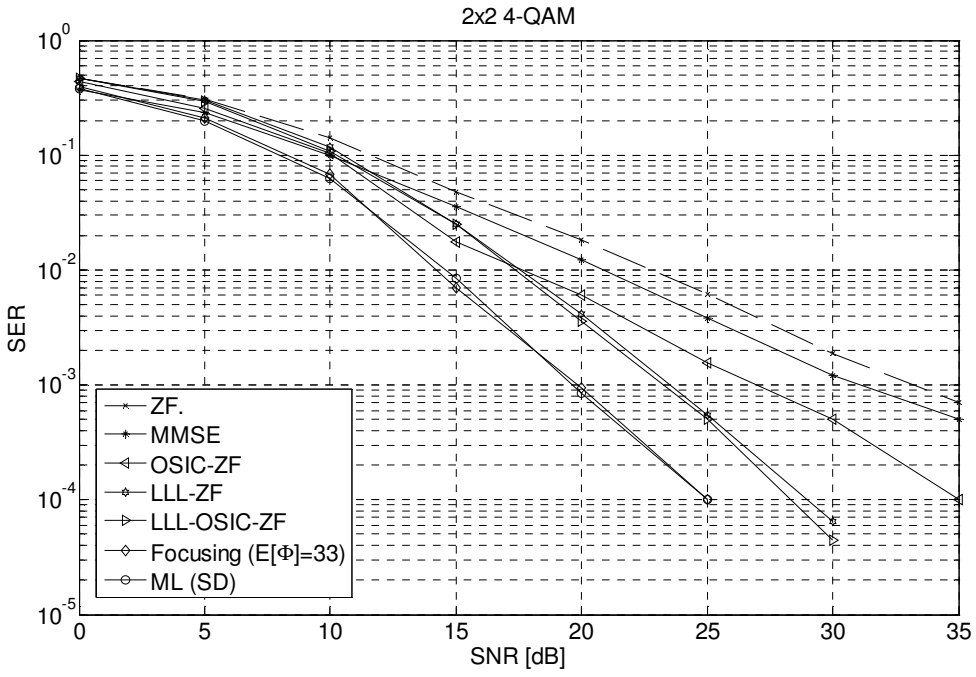


Figure 6.17: Detection in n=4 real dimensions (2×2 antennas) with QPSK.

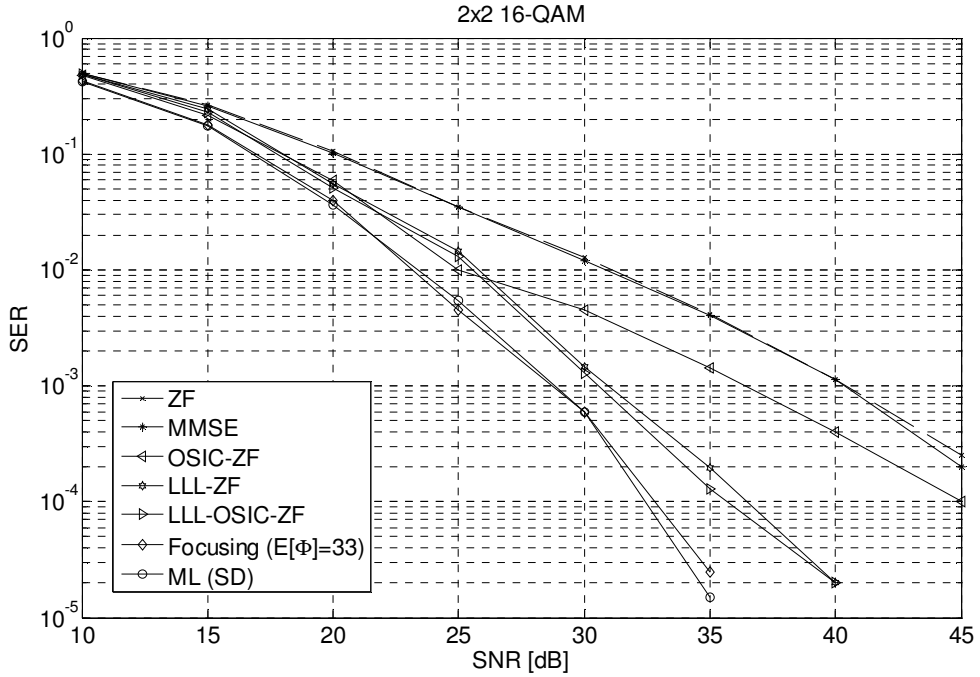


Figure 6.18: Detection in n=4 real dimensions (2×2 antennas) with 16-QAM.

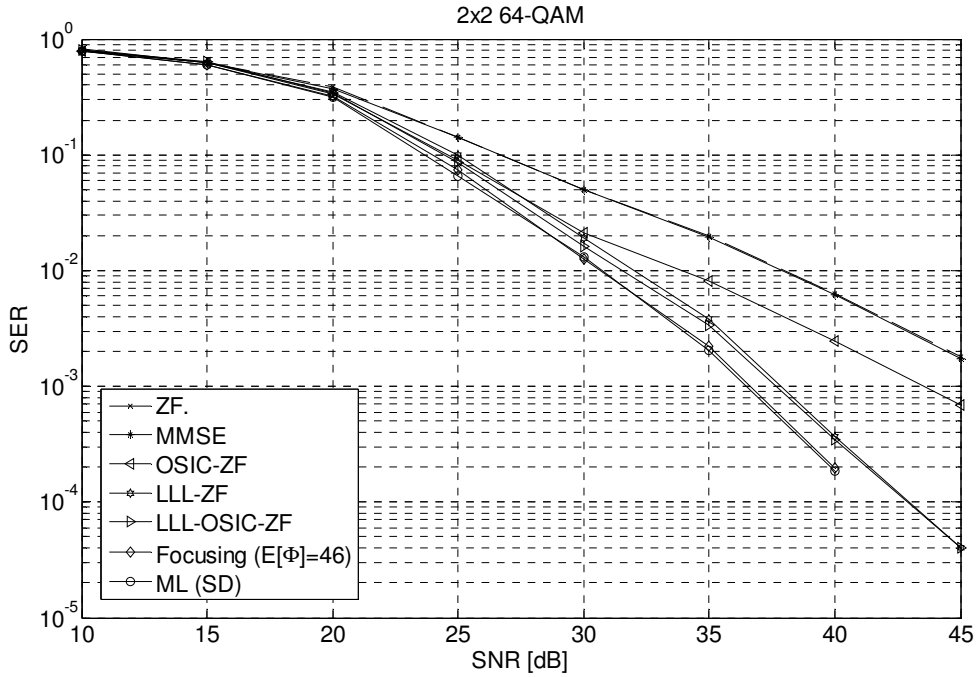


Figure 6.19: Detection in n=4 real dimensions (2×2 antennas) with 64-QAM.

6.6.2 — 3×3 Antennas

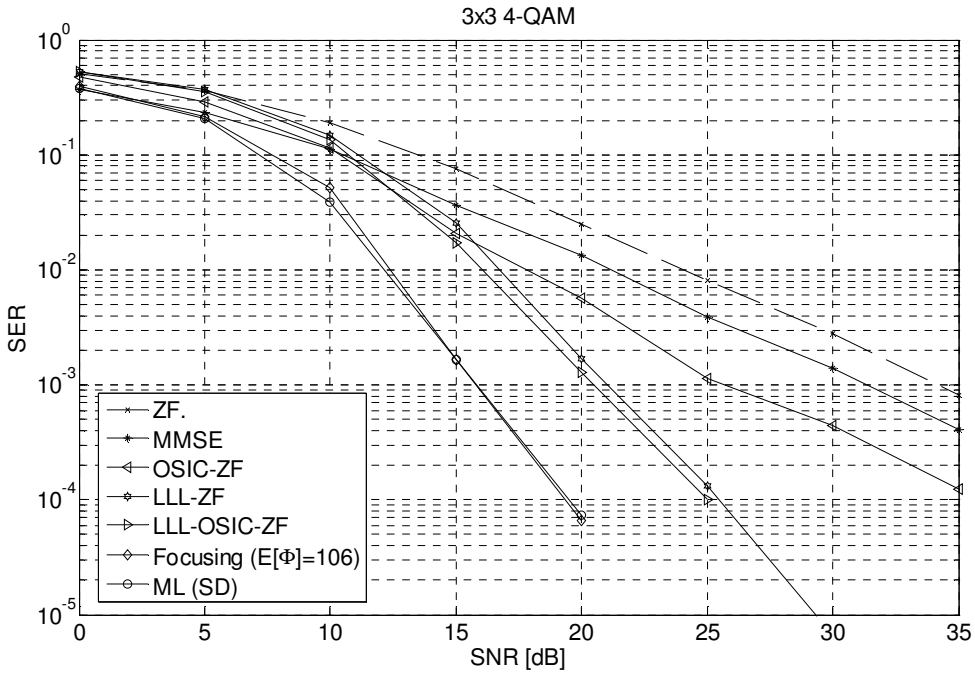


Figure 6.20: Detection in n=6 real dimensions (3×3 antennas) with QPSK.

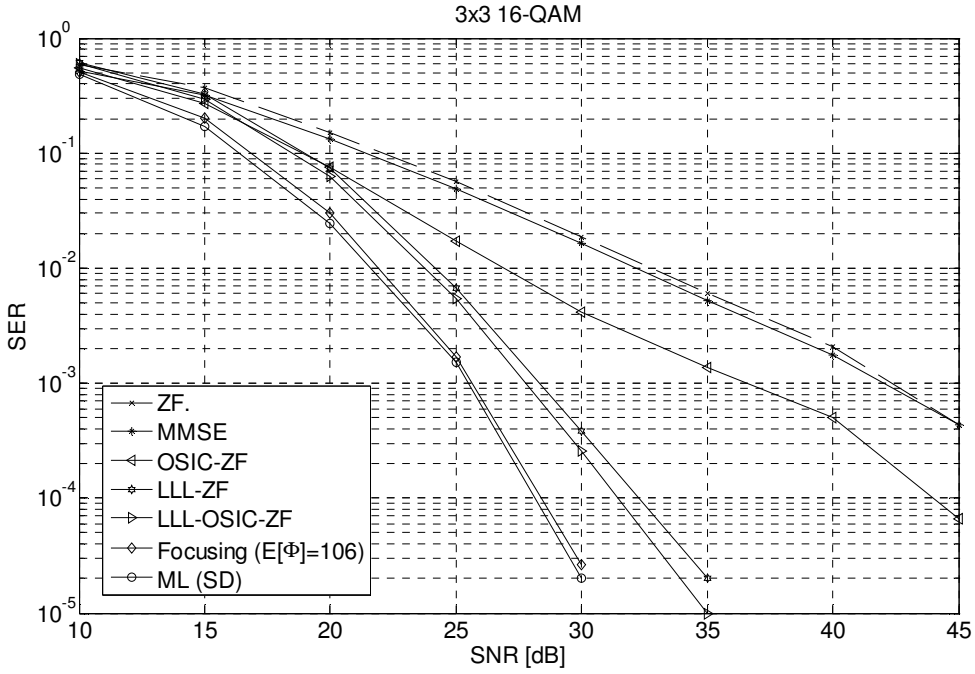


Figure 6.21: Detection in n=6 real dimensions (3×3 antennas) with 16-QAM.

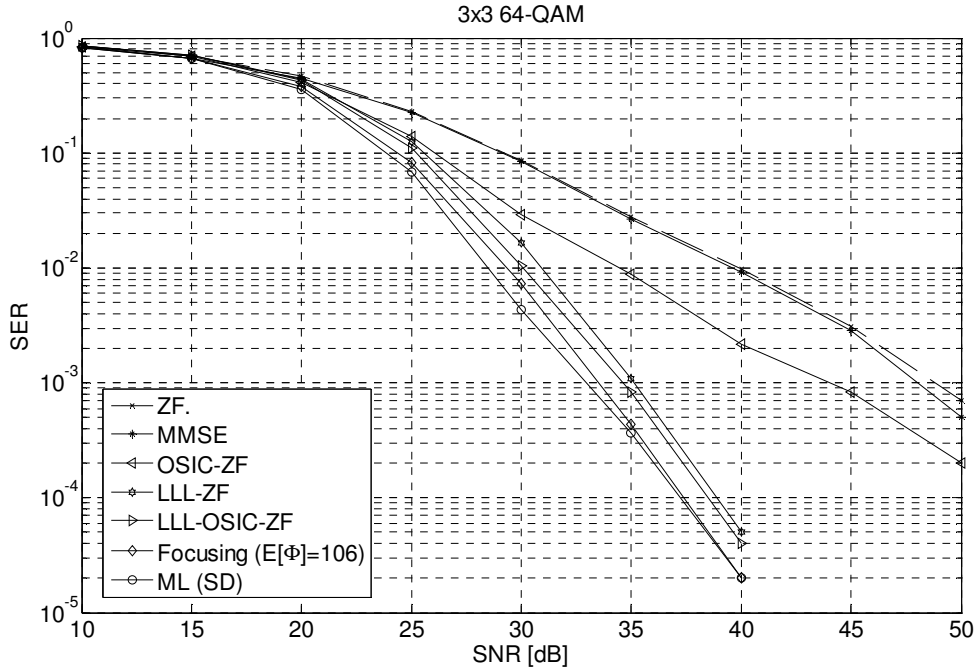


Figure 6.22: Detection in n=6 real dimensions (3×3 antennas) with 64-QAM.

6.6.3 — 4×4 Antennas

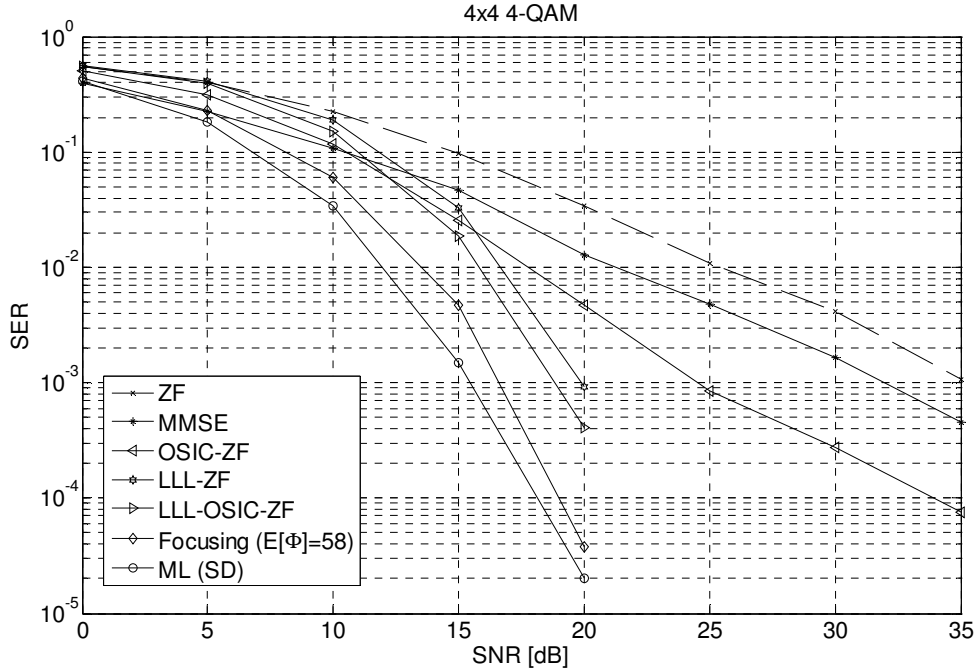


Figure 6.23: Detection in n=8 real dimensions (4×4 antennas) with QPSK.

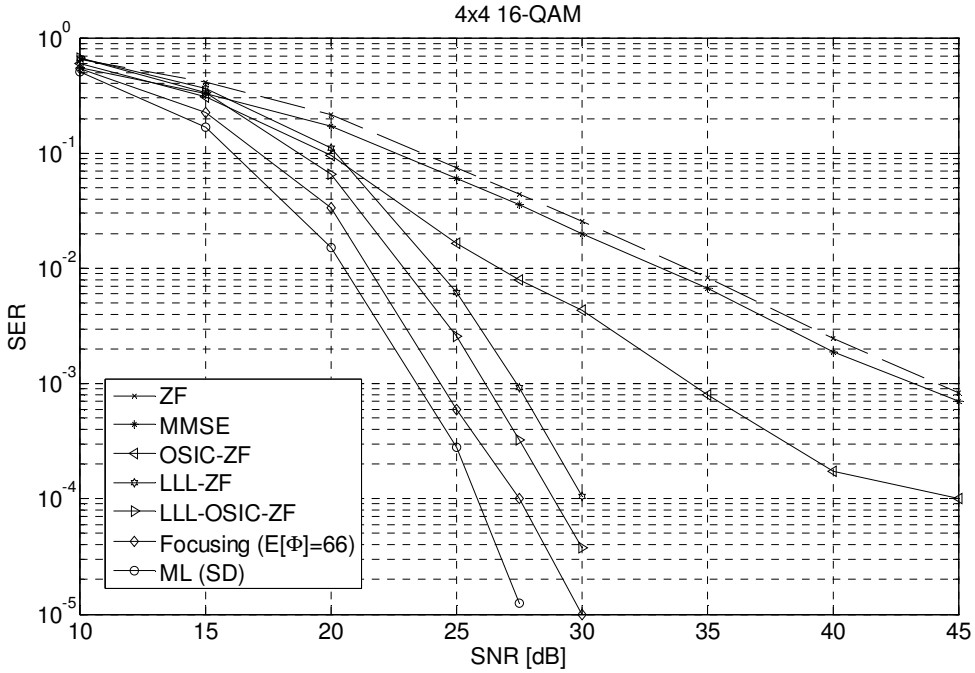


Figure 6.24: Detection in n=8 real dimensions (4×4 antennas) with 16-QAM.

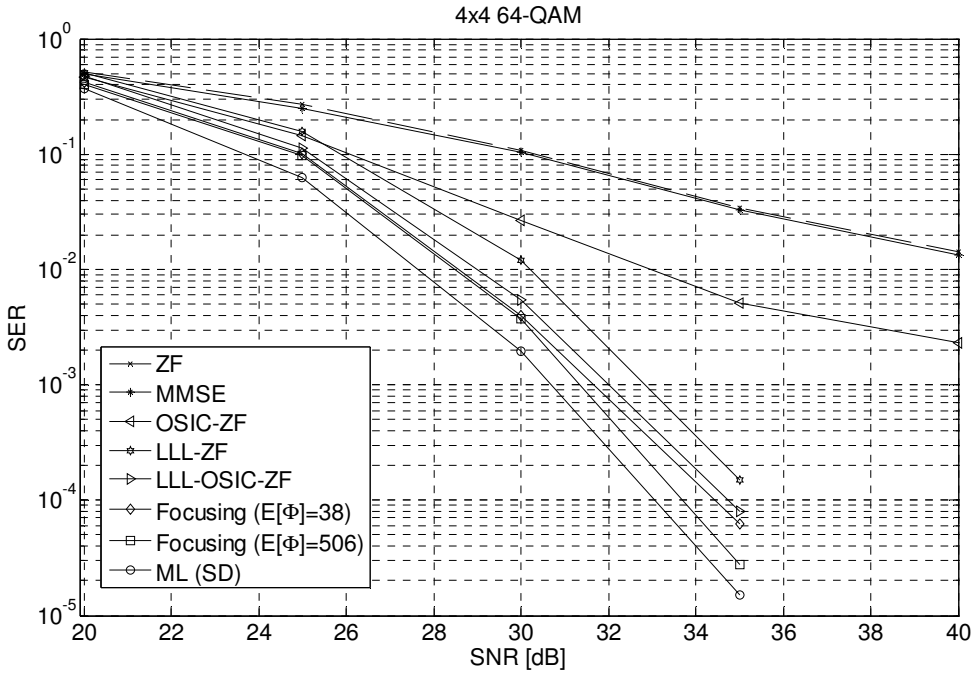


Figure 6.25: Detection in n=8 real dimensions (4×4 antennas) with 64-QAM.

6.6.4 — 6×6 Antennas

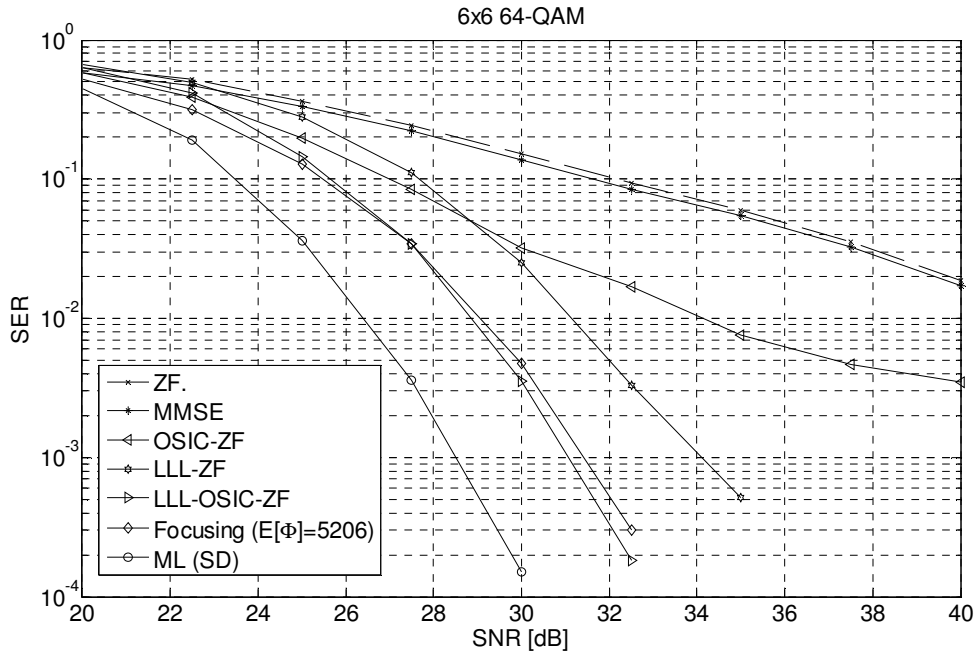


Figure 6.26: Detection in n=12 real dimensions (6×6 antennas) with 64-QAM.

6.7 — Discussion of the Results

Noticeably, the proposed receiver attains the full diversity provided by MLD, which until now was the distinctive characteristic of receivers with lattice-reduction pre-processing [173]. Moreover, the proposed trellis-based detection scheme reduces the gap between LRA and MLD performance, and the required number of cosets needed to achieve quasi-optimum detection is surprisingly small in configurations up to 4×4.

The maximum admissible number of cosets (i.e., paths in a trellis) is set to Γ in Algorithm 1. The simulations show that actually their average $E\{\Phi\}$ is, in most cases, about $\Gamma/2$.

Figure 6.25 shows the performance for 4×4 antennas with 64 QAM, which is a typical benchmark MIMO configuration. Limiting the admissible number of cosets to Γ=100, we observe that an average of 38 paths is enough to synthesise good approximated lattices in $\mathcal{L}_{\mathrm{R}}$ that achieve a performance about 1.2 dB away from MLD,

coinciding with the performance of LLL-OSIC-ZF. With an average of 506 cosets, the gap to MLD reduces to 0.6 dB.

For the 2×2 setup (from Figure 6.17 to Figure 6.19) quasi-optimum performance is always reached with a very low number of cosets (less than 50 for all modulations). In the 3×3 configuration, 106 cosets guarantees a quasi-optimum performance with all the modulations tested, although a small degradation can be noticed as the order of the modulation increases.

In the case of 12 real dimensions, the number of cosets required to outperform lattice-reduction with OSIC rises to over 5,000 (which is something that should be expected from the pdf shown in Figure 6.16).

In the simulations it was also observed that, in all cases when the performance approached the one of MLD, then the focusing transformation is $\mathcal{F} \approx \mathbf{I}$, which shows that the synthetic lattices in $\mathcal{L}_{\mathrm{R}}$ are close to the given lattice. Indeed, the distance $\left\|\mathcal{F}-\mathbf{I}\right\|_F$ constitutes a metric for the similarity between the lattices. This observation was verified graphically by visualising superimposed 2-dimensional slices of the original and the created synthetic lattices. This can be achieved by selecting a 2-dimensional sublattice generated by any pair of generator vectors and then plot the resulting 2D sublattice using a QR rotation to place the pair of generators onto the span of the first two dimensions of the space. Figure 6.27 shows an example of doing just this.

The number of cosets needed for near-optimal performance diminishes for smaller alphabets (smaller M). This happens because the distortion between the received lattice and the approximated lattice in $\mathcal{L}_R$ increases as one gets further away from the origin (as observed in Figure 6.27). It should also be noticed that, by construction, the number of trellis paths is an upper bound on the number of trellis states. Finally, note that the length of the trellises (number of segments) is determined by the dimensionality of the lattice ($n = 2N_T$) and therefore, for the typical number of antennas in MIMO, these trellises are rather short.

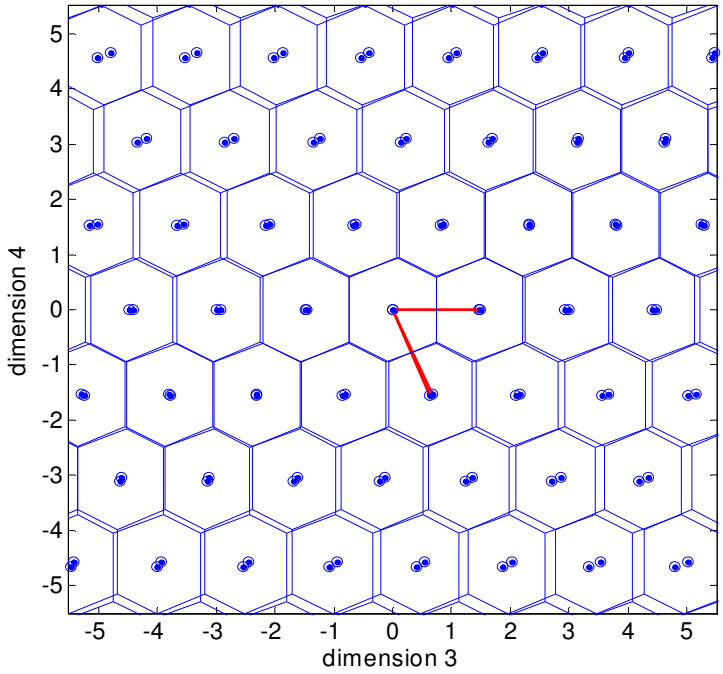
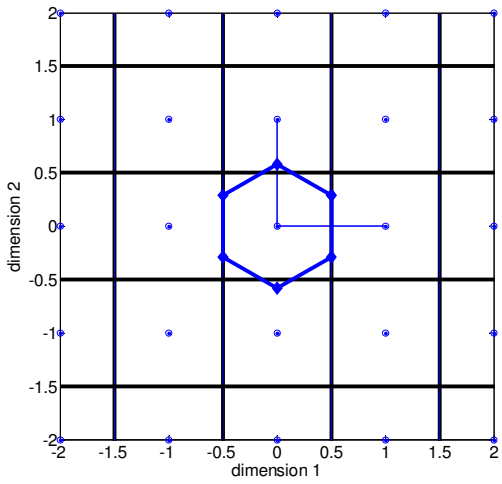


Figure 6.27: Slice of dimensions 3 and 4 of a 4-dimensional lattice overlapped with the nearest synthetic lattice found (with Φ=495 cosets). Both lattices are depicted together with their Voronoi regions.

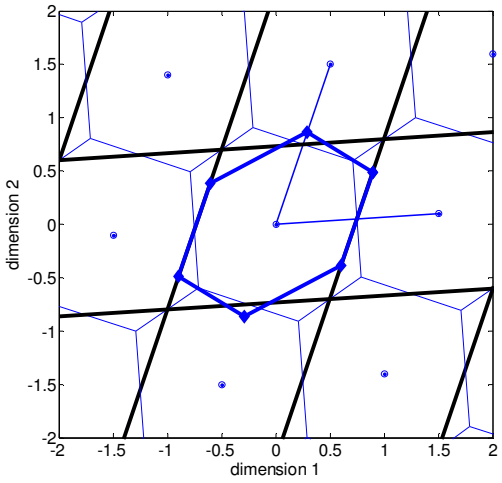
6.8 — Focusing Onto Fixed Lattices in $\mathcal{L}_R$

It is known that the optimal decision region for the cubic lattices $\mathbb{Z}^n$ coincide with the ones of ZF. However, for other lattices, the coverage of the MLD region that a linearly transformed hyper-cube achieves is very poor. One may ask if focusing onto a *fixed* lattice with a decision region with a shape closer to the n-hypersphere could, on average, result in a better coverage of the Voronoi regions. In that case, instead of creating a similar lattice with Algorithm 3.1 for every channel instance, the focusing operation could remain fixed and the linear transformation could focus, for example, onto the Schläfli lattice when working in 4D, or onto the Gosset lattice when working in 8D. They both have well known trellises and are denser than the cubic lattice in their respective dimensions, thus with Voronoi regions geometrically closer to an hypersphere than the cubic regions are [20].

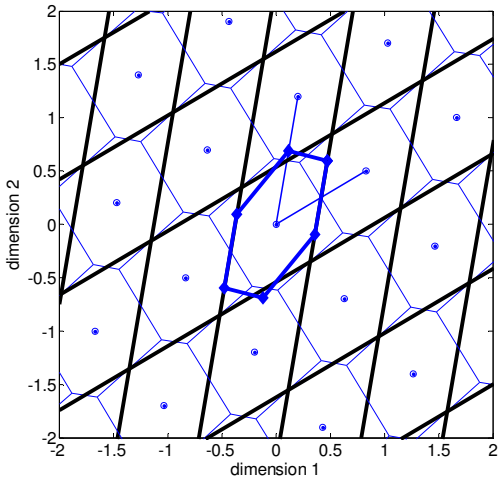
In order to assess this conjecture, simulations were conducted using the lattices D_4 and E_8 respectively for 2×2 and 4×4 configurations, and it was found that the performance results were no better than the one obtained with ZF. It is possible to shed light on the reason for this performance by visualising an example in 2D using the A_2 lattice (with an hexagonal fundamental region, as depicted in Figure 6.28).



(a) Lattice $\mathbb{Z}^2$ before the channel and the fundamental region of A_2 (blue).



(b) Case with $\mathbf{H}_1$.



(c) Case with $\mathbf{H}_2$.

Figure 6.28: Comparison of the ZF decision region with the one corresponding to a focusing onto A_2. ML (thin blue), Zero forcing (black) and image of the hexagonal fundamental region of A_2

In Figure 6.28 it is possible to observe the deformation of the fundamental hexagon on A_2 when it undergoes the linear transformations

$$\mathbf{H}_1 = \begin{bmatrix} 3/2 & 1/2 \\ 1/10 & 3/2 \end{bmatrix} \quad \text{and} \quad \mathbf{H}_2 = \begin{bmatrix} 5/6 & 1/5 \\ 1/2 & 6/5 \end{bmatrix}. \tag{6.19}$$

With this example, it can be perceived that having a decision region with six sides instead of four does not necessarily result in a better coverage of the Voronoi region. In fact, the coverage may become reduced and the ZF region may offer better coverage of the MLD region.

6.9 — Summary

In this chapter a new detection concept was proposed for MIMO. The concept revisits the channel inversion technique and generalises it to the concept of focusing the received lattice onto a lattice geometrically similar to it, but whose special structure allows a simple detection technique. It was shown that it is possible to well approximate typical lattices in MIMO by lattices with an orthogonal quotient group, which allow a trellis representation.

Detection on these lattices attains quasi-optimal performance while maintaining a reasonably low complexity for systems up to 4×4 utilising 64QAM, however a 6×6 system again using 64QAM is probably beyond the practical limit for the proposed technique. The receiver also captures the full diversity that exists in the SM channel, which is a much sought property. Moreover, it exhibits a performance gain in comparison to LRA.

The results presented are non-constructive, meaning that even though the existence of those lattices is proven and their performance is assessed, the construction of the trellis remains an open problem for rational lattices owning to the numerical problems when computing their Hermite normal form.

Chapter 7 – Closed Loop Spatial Multiplexing

While the previous chapters dealt with open loop SM, i.e., when the transmitter has no information about the matrix channel $\mathbf{H}$. In contrast, this chapter proposes a close loop system that is an alternative to the traditional one base on the singular value decomposition.

As it was seen in Chapter 2, to obtain the Gram matrix associated with a given generator matrix is a trivial operation, the converse is not obvious for non-square matrices and is a research topic in algorithmic number theory. This chapter proposes a method to execute such a conversion and applies it to a feedback technique that removes some of the complexity from the receiver to the transmit side.

7.1 – Feedback in MIMO

As seen in chapters 5 and 6, there are several ways of describing a lattice (e.g., via modular equations [136] or by trellis structures [227]). Nevertheless, the two most common forms of specifying a lattice in engineering applications are *i)* the generator matrix and *ii)* the Gram matrix. While the computation of the latter given the former is trivial, the reverse operation is not, and an efficient algorithm for this conversion remains an open problem in lattice theory.

It should be noted that if efficient algorithm for this reverse operation existed, the lattice could be described using only about half the number of elements of $\mathbf{H}$, since the Gram matrix is always symmetric. For example, in MIMO communications with CSIT, this means that about half the number of coefficients would need to be sent to the Tx when compared with that in traditional feedback [99]. Using the traditional example in [99] , while in a single-input single-output configuration (with BPSK modulation) the channel state information is conveyed by one coefficient only, in a 4×4 antenna system one has 16 complex variables describing the channel, or equivalently 32 real coefficients, that need to be periodically fedback to the transmitter. In fact, the number of coefficients to be fedback is the product of the number of antennas at the transmitter, at the Rx, the delay spread and, in multi-user environments, also proportional to the product with the number of users.

The chapter proposes a technique to obtain a close approximation for a generator matrix given a Gram matrix of a lattice. The algorithm is based on an exact technique recently proposed by Lenstra [103] (an historical figure in the fields of lattice algorithms).

7.2 — The Matrix Conversion Method

Given a rational Gram matrix $\mathbf{G}$ it is possible to diagonalise the quadratic form as

$$\mathbf{G} = \mathbf{L} \cdot \mathbf{D} \cdot \mathbf{L}^T , \tag{7.1}$$

where $\mathbf{L}$ is a rational $n \times n$ lower triangular matrix with ones in the diagonal (i.e., is a unit matrix) and $\mathbf{D}$ is a $n \times n$ diagonal matrix with rational diagonal entries $d_{jj} > 0$.

The first step is to expand these $d_{jj} \in \mathbb{Q}$ into a sum of a fixed number of squares of R rational numbers, that is,

$$\tilde{d}_{jj} = z_{j,1}^2 + z_{j,2}^2 + \cdots z_{j,R}^2 . \tag{7.2}$$

An exact expansion of these d_{jj} can be accomplished by applying a naive greedy algorithm as proposed for the first time by Lenstra in [103]. Imposing an exact expansion for each d_{jj} often leads to a large number of terms in the sum (7.2) and for

that reason Lenstra also proposed the use of a randomized algorithm given in [228], which assures the bound $R \leq 4$.

In this section one proposes to replace an exact conversion from $\mathbf{G}$ to $\mathbf{H}$ by an approximate conversion (leading to a $\tilde{\mathbf{H}}$) using a fixed complexity algorithm that can be applied in a real time communication system. Based on the results in [228], a simple greedy algorithm is used for the expansion and truncate the number of terms to $R \leq 4$ leading to a *truncated Lenstra algorithm*. One way of achieving this is by using R equal terms in (7.2). One may notice that when R=1, the algorithm resorts to an approximated Cholesky decomposition.

One starts by constructing a *tall matrix* $\mathbf{B}$ with $R \cdot n$ rows and n columns. For the case with R=4 terms for each of the d_{jj}, $\mathbf{B}$ has the form

$$\mathbf{B} = \begin{bmatrix} z_{1,1} & z_{1,2} & z_{1,3} & z_{1,4} & \ddots & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & & z_{j,1} & z_{j,2} & z_{j,3} & z_{j,4} & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & & z_{n,3} & z_{n,4} \end{bmatrix}^T \tag{7.3}$$

where each row has one and only one non-zero entry. Now, one can re-construct the diagonal matrix $\mathbf{D}$ from $\mathbf{B}$ using

$$\tilde{\mathbf{D}} = \mathbf{B}^T \mathbf{B}.$$

This matrix multiplication was made explicit to emphasise how this ensures that each d_{jj} is a sum of squares as defined in (7.2). Finally, the approximated generator matrix can be seen to be

$$\tilde{\mathbf{H}} = \mathbf{B} \cdot \mathbf{L}^T, \tag{7.4}$$

because

$$\begin{aligned} \tilde{\mathbf{G}} &= \mathbf{L} \cdot \tilde{\mathbf{D}} \cdot \mathbf{L}^T = \mathbf{L} \cdot \mathbf{B}^T \cdot \mathbf{B} \cdot \mathbf{L}^T \\ &= \left(\mathbf{B} \cdot \mathbf{L}^T \right)^T \cdot \mathbf{B} \cdot \mathbf{L}^T = \tilde{\mathbf{H}}^T \cdot \tilde{\mathbf{H}}, \end{aligned} \tag{7.5}$$

which verifies (2.4) (defined in Chapter 2).

The complexity of this technique is cubic in the dimension n, due to the $\mathbf{LDL}^T$ steps, to which one should add $\mathcal{O}\left(n\right)$ for the rational approximation steps. The overall

complexity is $\mathcal{O}\left(n^3+n\right)$, however, as it will be shown later in Table 7.1, as the $\mathbf{LDL}^T$ decomposition will be reused, only the n term will add to the complexity of the technique to be presented.

It should be noted that, unlike Cholesky decomposition, this technique is applicable to both square and non-square matrices, allowing us to retrieve a rectangular $\mathbf{H}$ from $\mathbf{G}$.

7.3 — Closed Loop Technique

Using traditional singular value decomposition (SVD), [148], [229] one has

$$\begin{aligned}\mathbf{y} &= \underbrace{\mathbf{U}\Sigma\mathbf{V}^T}_{\mathbf{H}}\mathbf{x}+\mathbf{n}\\ \underbrace{\mathbf{U}^T\mathbf{y}}_{\mathbf{y}_d} &= \mathbf{U}^T\mathbf{U}\Sigma\mathbf{V}^T\left(\mathbf{V}\mathbf{x}\right)+\mathbf{U}^T\mathbf{n}=\Sigma\cdot\mathbf{x}+\mathbf{U}^T\mathbf{n}\end{aligned} \tag{7.6}$$

where $\Sigma$is a diagonal matrix and $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices or orthogonal, if the real equivalent model is used. It should be emphasised that, as these rigid transformations are norm-preserving rotations, the term $\mathbf{U}^T\mathbf{n}$ preserves the statistics of the noise term $\mathbf{n}$. The traditional SVD-based scheme implies one SVD decomposition (requiring at least $\mathcal{O}(6n^3)$ flops [229]) at the Rx in addition to matrix multiplications both at the Rx and at the Tx (each multiplication requiring $\mathcal{O}(n^3)$ flops). As it was mentioned in Chapter 1, this technique achieves capacity when using the *water filling* power allocation technique, which allocates more power to the streams associated with larger singular values of $\mathbf{H}$ [35].

It has been shown in [230] that the $\mathbf{LDL}^T$ decomposition achieves better performance than standard SVD, while being slightly less complex. Most importantly, that new approach takes advantage of having a precoding matrix with $(n^2-n)/2$ zero elements. In fact, it requires lower triangular precoder instead of the unitary $\mathbf{V}$ in (7.6). That lower triangular matrix is fedback from the Rx to the Tx, saving bandwidth in the feedback channel.

This chapter proposes a technique with similar performance to the one in [230] but that removes most of the complexity from the Rx side to the Tx side, which is relevant in scenarios where the Tx is a BS and the Rx should be made simple.

Remark: since the objective in this chapter is not to assess the capacity-achieving regime so, for simplicity, uniform power is allocated to the transmit antennas.

Both the contribution in this chapter and the one in[230] have a pre-processing stage at Rx consisting of the generation of a definite positive matrix $\mathbf{G}$, that is the Gram matrix of the lattice defined by the columns of $\mathbf{H}$.

In this proposal it is mandatory that CSIT exists so that the Tx is able to construct the precoding matrix $\mathbf{P}$. This chapter shows that his can be achieved with the feedback of a lower triangular matrix only. Given the symmetry of $\mathbf{G}$, the Tx only needs to receive $(n^2+n)/2$ coefficients and from them is able to reconstruct the entire matrix, achieving the same bandwidth savings seen in [230] for the feedback channel. After reconstructing the entire $\mathbf{G}$ (by symmetry), the Tx can use the truncated Lenstra algorithm described in Section 7.2 to obtain an equivalent generator matrix for the lattice. This matrix, $\tilde{\mathbf{H}}$, is not the same as $\mathbf{H}$ but rather an equivalent generator matrix for the lattice, holding the same Gram matrix. However, it is possible to obtain from them both the unique generator matrix resulting from QR decompositions remembering that a QR decomposition is unique when imposing the positiveness of elements in the main diagonal. Thus

$$\mathbf{H} = \mathbf{QR} \text{ and } \tilde{\mathbf{H}} = \tilde{\mathbf{Q}}\tilde{\mathbf{R}} \tag{7.7}$$

lead to $\mathbf{R}$ and $\tilde{\mathbf{R}}$, which would be the same matrix (up signs in main diagonal) if there was no distortion associated with $\tilde{\mathbf{H}}$ in the truncated Lenstra algorithm. A key aspect is that the same Gram matrix is also obtainable from $\mathbf{R}$ alone, $\tilde{\mathbf{R}}$ alone or even a mixture of both, given their closeness:

$$\mathbf{G} = \mathbf{R}^T\mathbf{R} \cong \tilde{\mathbf{R}}^T\tilde{\mathbf{R}} \cong \mathbf{R}^T\tilde{\mathbf{R}}\,. \tag{7.8}$$

As seen previously, $\mathbf{G}$ has an $\mathbf{LDL}^T$ decomposition, which can be calculated not only given $\mathbf{H}$ or $\tilde{\mathbf{H}}$ but also given $\mathbf{R}$, or $\tilde{\mathbf{R}}$, or both. However, this is not the matrix that is to be $\mathbf{LDL}^T$ decomposed. One starts by applying a QR decomposition, so that

$$\mathbf{y} = \mathbf{Q}\,\mathbf{R}\,\mathbf{x} + \mathbf{n}\,. \tag{7.9}$$

Then, defining the precoding matrix $\mathbf{P} = \tilde{\mathbf{R}}^T(\tilde{\mathbf{L}}^T)^{-1}\tilde{\mathbf{D}}^{-1/2}$,

$$\mathbf{y}' = \mathbf{Q}\underbrace{\mathbf{R}\,(\tilde{\mathbf{R}}^T}_{\mathbf{G}'}\,(\tilde{\mathbf{L}}^T)^{-1}\tilde{\mathbf{D}}^{-1/2})\,\mathbf{x} + \mathbf{n}\,. \tag{7.10}$$

The matrices used in (7.10) will be presented and justified in the following. First, notice that this caused a matrix $\mathbf{G}' = \mathbf{R}\tilde{\mathbf{R}}^T$ to appear (a permutation matrix may be needed together with $\tilde{\mathbf{R}}$ to have a unique QR), which, despite not being the Gram matrix of the underlying lattice, it is the (approximate) Gram matrix of the lattice spanned by the row lattice. This matrix $\mathbf{G}'$ also has an $\mathbf{LDL}^T$ decomposition and thus (7.10) can equivalently be written as

$$\mathbf{y}' = \mathbf{Q}\underbrace{\tilde{\mathbf{L}}\,\tilde{\mathbf{D}}\,\tilde{\mathbf{L}}^T}_{\mathbf{G}'}\,(\tilde{\mathbf{L}}^T)^{-1}\,\tilde{\mathbf{D}}^{-1/2}\,\mathbf{x} + \mathbf{n}\,. \tag{7.11}$$

Finally, after the detection filter at the receiver, the entire chain becomes

$$\begin{aligned} \underbrace{\left(\tilde{\mathbf{L}}^{-1}\mathbf{Q}^{-1}\right)\mathbf{y}'}_{\mathbf{y}'_d} &= \left(\tilde{\mathbf{L}}^{-1}\mathbf{Q}^{-1}\right)\mathbf{Q}\,\tilde{\mathbf{L}}\,\tilde{\mathbf{D}}\,\tilde{\mathbf{L}}^T\,(\tilde{\mathbf{L}}^T)^{-1}\,\tilde{\mathbf{D}}^{-1/2}\,\mathbf{x} + \left(\tilde{\mathbf{L}}^{-1}\mathbf{Q}^{-1}\right)\mathbf{n} \\ \mathbf{y}'_d &= \tilde{\mathbf{D}}\tilde{\mathbf{D}}^{-1/2}\cdot\mathbf{x} + \left(\tilde{\mathbf{L}}^{-1}\mathbf{Q}^T\right)\mathbf{n} = \mathbf{D}_{eq}\cdot\mathbf{x} + \underbrace{\left(\tilde{\mathbf{L}}^{-1}\mathbf{Q}^T\right)\mathbf{n}}_{n_d} \end{aligned} \tag{7.12}$$

It should be noted that, since $\mathbf{Q}$ is orthogonal (unitary if considering complex models), then $\mathbf{Q}^{-1} = \mathbf{Q}^T$, which further simplifies the computations at the Rx, which now only has to apply the filtering $\mathbf{F} = \tilde{\mathbf{L}}^{-1}\mathbf{Q}^T$ to the incoming precoded signal (i.e., the unavoidable filtering multiplications that are present in all detectors). Besides that, the Rx only needs to compute $\mathbf{G}$ and (given its symmetry) send back to the Tx only the lower or the upper parts of $\mathbf{G}$, which will be denoted by $\mathbf{G}_{1/2}$. Moreover, both $\tilde{\mathbf{L}}^{-1}$ and $\mathbf{Q}^T$ are computed and sent from the Tx to the Rx.

The resulting transmission chain (7.12) can be interpreted in two ways: *i)* algebraically it corresponds to a set of independent transmission channels and *ii)* geometrically it corresponds to a communication problem over a rectangular lattice as the diagonal matrix $\mathbf{D}_{eq}$ corresponds to a set of orthogonal generating vectors. The better performance can be geometrically interpreted from this insight. A rectangular lattice is obtained from a deformation of a cubic lattice $\mathbb{Z}^n$ by stretching each dimension according to each d_{jj}. Its decision regions are hyper-rectangles and for that reason even a ZF detection experiences no performance penalty.

The right multiplication of the channel matrix by $\tilde{\mathbf{R}}^T$ in (7.9) changes the power at the transmitter. The geometric interpretation is also useful on this matter. The "row lattice" $\mathcal{L}(\mathbf{H}^T)$ has volume

$$\mathrm{Vol}\left(\mathcal{L}(\tilde{\mathbf{R}}^T)=\right)\sqrt{\det\left(\tilde{\mathbf{R}}\tilde{\mathbf{R}}^T\right)}. \tag{7.13}$$

At the same time, because $\tilde{\mathbf{L}}$ and $\tilde{\mathbf{L}}^T$ are unit matrices,

$$\begin{aligned}\mathrm{Vol}\left(\mathcal{L}(\tilde{\mathbf{D}})\right)&=\det\left(\tilde{\mathbf{D}}\right)=\det\left(\tilde{\mathbf{L}}\tilde{\mathbf{D}}\tilde{\mathbf{L}}^T\right)\\&=\det\left(\tilde{\mathbf{G}}'\right)=\det\left(\tilde{\mathbf{R}}\tilde{\mathbf{R}}^T\right).\end{aligned} \tag{7.14}$$

Subsequently, one also needs the insertion of a diagonal scaling $\mathbf{D}^{-1/2}$ at the precoding stage so that the volume of both lattices underlying the transmission scheme becomes the same.

Figure 7.1 depicts the overall transmission scheme that is proposed while in Figure 7.2 and in Figure 7.3 one can observe in detail the processing required respectively at the Tx and at the Rx as well as the fluxes of CSI between both of them.

At the Rx it is important to highlight that there are two parallel operations running simultaneously, each one associated with a different fading block: *i)* obtain $\mathbf{G}$ that will be sent back to Tx in the form of a triangular matrix and *ii)* construct the receive filter from a received strictly upper triangular matrix and $\mathbf{Q}$. In fact, $\tilde{\mathbf{L}}^{-1}$ is not only a lower triangular but also a unit lower triangular (ones in the diagonal). This saves the transmission of the diagonal and thus only the $(n^2-n)/2$ coefficients of $\tilde{\mathbf{L}}^{-1}$ are needed

to be forwarded to the Rx. These coefficients are denoted by $\tilde{\mathbf{L}}_u^{-1}$. The process is summarised in Algorithm 1. (The channel is assumed to remain unchanged between adjacent symbols as it is common in the slow fading assumption.)

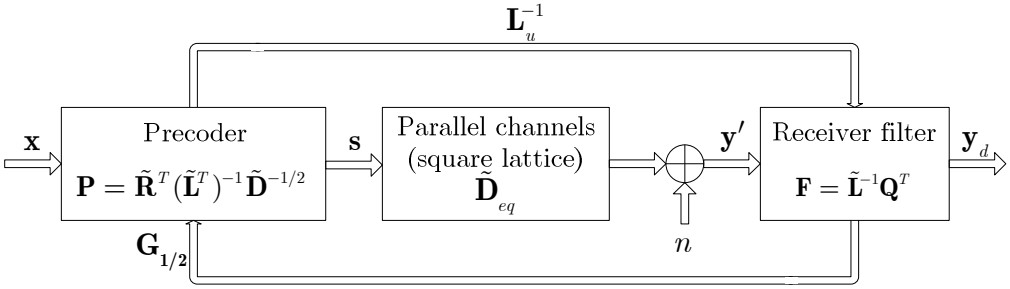


Figure 7.1: Proposed closed loop transmission scheme.

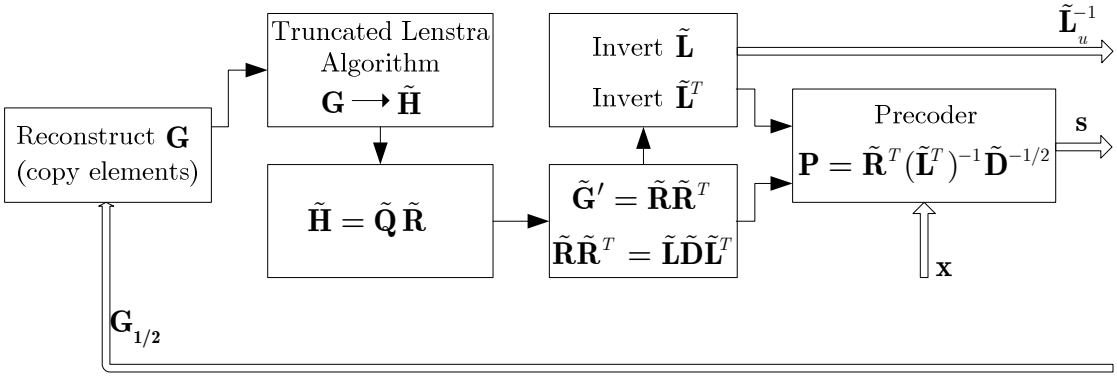


Figure 7.2: Processing at the transmitter.

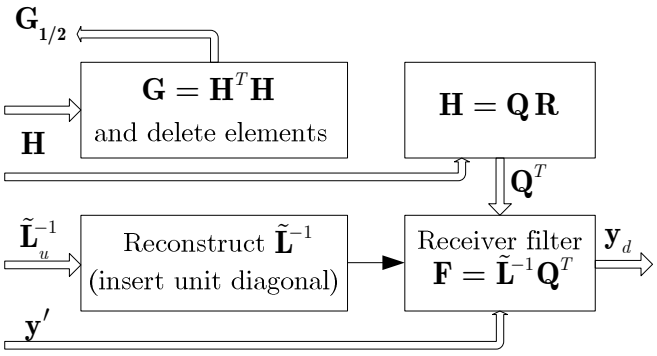


Figure 7.3: Processing at the receiver.

ALGORITHM 7.1 CLOSED LOOP TECHNIQUE

1: Channel estimation at Rx : $\mathbf{H}$

2: Gram matrix of the lattice at Rx : $\mathbf{G} = \mathbf{H}^T\mathbf{H}$

3: Lower triangular matrix is fedback: $\mathbf{G}_{1/2}$ (Rx$\rightarrow$ Tx)

4: Gram matrix is reconstructed at Tx:

$$\mathbf{G} = \mathbf{G}_{1/2} + \left(\mathbf{G}_{1/2}\right)^T - \mathrm{diag}\left(\mathbf{G}_{1/2}\right)$$

5: Obtain approximate $\tilde{\mathbf{H}}$ from $\mathbf{G}$ using the algorithm in Section 7.2 (which encompasses a $\mathbf{LDL}^T$ for $\mathbf{G}$)

6: Compute QR decomposition of $\tilde{\mathbf{H}}$: $\tilde{\mathbf{H}} = \tilde{\mathbf{Q}}\tilde{\mathbf{R}}$

7: Compute the Gram matrix of the "row lattice" at Tx: $\tilde{\mathbf{G}}' = \tilde{\mathbf{R}}\tilde{\mathbf{R}}^T$

8: Decomposition of $\mathbf{G}'$ at Tx: $\tilde{\mathbf{G}}' = \tilde{\mathbf{L}}\tilde{\mathbf{D}}\tilde{\mathbf{L}}^T$

9: Precoding at Tx: $\mathbf{P} = \tilde{\mathbf{R}}^T(\tilde{\mathbf{L}}^T)^{-1}\tilde{\mathbf{D}}^{-1/2}$; $\mathbf{s}$ is sent (note: for a non-squared $\tilde{\mathbf{R}}$ the non-zero rows must be deleted)

10: Strictly lower triangular matrix is sent: $\tilde{\mathbf{L}}_u^{-1}$ (Tx$\rightarrow$ Rx)

11: Compute QR decomposition of $\mathbf{H}$: $\mathbf{H} = \mathbf{QR}$ (note: can be computed at the same time as steps 4-10)

12: $\tilde{\mathbf{L}}^{-1}$ is reconstructed at Rx: $\tilde{\mathbf{L}}^{-1} = \tilde{\mathbf{L}}_u^{-1} + \mathbf{I}_{n\times n}$

13: Receiver filter $\mathbf{F} = \tilde{\mathbf{L}}^{-1}\mathbf{Q}^T$ multiplies the received chain and the received vector becomes $\mathbf{y}_d = \tilde{\mathbf{D}}^{1/2}\mathbf{x} + \mathbf{n}_d$

The number of flops required by the $\mathbf{LDL}^T$ decomposition is $\mathcal{O}(n^3/3)$, which is half of the number of flops needed in Gaussian elimination, the number of flops of QR decomposition is $\mathcal{O}(2n^3)$, and for the standard matrix multiplication one has $\mathcal{O}(n^3)$ [148], [229] (however, there are more efficient algorithms for matrix multiplication). Table 7.1 contains a comparison of the proposed technique with SVD and with [230] in terms of the number of flops and number of coefficients flowing in both the uplink and downlink. The number of operations in Table 7.1 is presented in a way that shows the contribution of each individual processing stage to the total number of operations of the Rx or Tx (matrix multiplications are counted as only one $\mathcal{O}(n^3)$ though). The complexity at the receiver comes from a QR decomposition and two matrix

multiplications: one to initially obtain $\mathbf{G}$ (similar to [230]) and then the unavoidable filtering multiplication by $\mathbf{F}$. One should remember that this last multiplication is common to all types of receivers in both closed or open-loop configurations.

Table 7.1: Comparison of the complexities of the schemes

	SVD	[230]	Proposal
# flops at Rx	$\mathcal{O}\left(4n^3 + n^3\right)$	$\mathcal{O}\left(n^3 + n^3/3 + n^3\right)$	$O\left(2n^3 + n^3\right)$
# flops at Tx	$\mathcal{O}\left(n^3\right)$	$\mathcal{O}\left(n^3\right)$	$O\begin{pmatrix} n + 2n^3 + \\ n^3/3 + n^3 \end{pmatrix}$
Coefficients in feedback	n^2	$\left(n^2 + n\right)/2$	$\left(n^2 + n\right)/2$
Coefficients in downlink	–	–	$\left(n^2 - n\right)/2$
Total of coefficients	n^2	$\left(n^2 + n\right)/2$	n^2

7.4 — Assessment of the Approximation

In order to access the approximation one first computes the error matrix of the Gram matrix involved (i.e., the Gram matrix associated with the "row lattice", as indicated in Section 7.3)

$$\mathbf{E} = \mathbf{G}' - \bar{\mathbf{G}}' \tag{7.15}$$

and one applies to it the squared *Frobenius matrix norm* [229]

$$\left\|\mathbf{E}\right\|_F^2 = \sum_{i,j} \left|e_{i,j}\right|^2 = \text{Trace}\left(\mathbf{E}^H \mathbf{E}\right) \tag{7.16}$$

as the evaluation metric.

Figure 7.4 shows the distribution of this error for three example cases having the number of real dimensions most common in MIMO wireless communications (and with variance 0.5 per real component).

Notice that despite the Gram matrix of the "row lattice" and the one of "column lattice" being different, they hold the same distribution because $\mathbf{H}$ and $\mathbf{H}^H$ exhibit the same statistics and consequently they are interchangeable in expression (2.4).

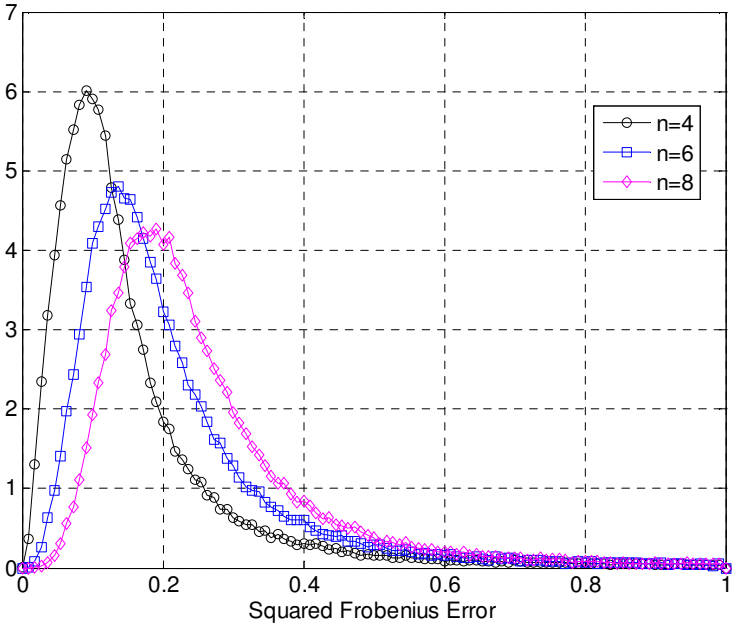


Figure 7.4: Probability distribution of the squared Frobenius norm of the error matrix for $\tilde{\mathbf{G}}$ (or $\tilde{\mathbf{G}}'$).

For a N_T=4, N_R=4 configuration (i.e., n=8 dimensions) under a Rayleigh fading channel and using 16-QAM modulation, the proposed $\mathbf{LDL}^T$ decomposition leads to the error shown in Figure 7.4, which contributes to negligible performance penalty in respect to the results presented in [230] for the same configuration and using the same MMSE receiver.

7.5 — Summary

This chapter starts by proposing a method to reconstruct a generator matrix of a lattice from one given Gram matrix of the same lattice for non-square matrices. Notice that for square matrixes one may use the Cholesky decompositions. Subsequently, the chapter presented a technique for channel diagonalisation of MIMO systems. With this technique: *i)* $\mathbf{LDL}^T$ decomposition takes place at the transmit side; *ii)* the number of elements to be fedback to Tx is $(n^2+n)/2$, as in [230]; *iii)* the filtering matrix at Rx is build from a unit lower triangular and an orthogonal matrix, which further reduces the

complexity of the filtering matrix multiplication at Rx. The extra cost to bear is a QR decomposition at the Rx. However, a QR module would have to exist at Rx if typical open-loop spatial multiplexing schemes are also to be supported. For large number of antennas, the presented closed loop architecture (i.e., with CSIT) for MIMO communications nearly halves the number of coefficients traditionally needed to represent the channel.

Chapter 8 – Conclusions

In the past few years, we have witnessed a period of vibrant new discoveries. Decades-long open problems have been solved, either exactly or via good engineering approximations. The mathematical techniques that form the foundation of our discipline, such as random coding, superposition coding, successive interference cancellation, lattice coding and quantization, binning (or hashing), linear and non-linear precoding, opportunistic scheduling and many more, are now at the heart of core technology developments, and are migrating into new systems and communication standards. (...) It is by now clear that the single-source single-link problem has arrived at a point where the marginal improvement, in most settings of engineering significance, is relatively small. In contrast, as soon as the problems are enriched with network aspects, such as distributed and correlated sources, interference and intermediate nodes that are neither sources nor destinations, the distance between theory and practice is still large, and the margins for dramatic improvements are potentially huge. Furthermore, even the theory offers plenty of long-standing or new open problems that will keep generations of information theorists busy for a long time. (...) there is still a lot of work to do!

Giuseppe Caire, 2011
In the *president's column* of [231]

8.1 – Research Contributions

In general, lattice problems are simple to describe but rather hard to solve optimally. In this dissertation several suboptimal solutions have been described for the closest vector problem, which is central in MIMO communication systems. This thesis started by placing SM in the context of MIMO in Chapter 1. Then, in Chapter 2, the

detection problem was framed as a CVP in real lattices. When describing the fundamental properties of lattices, this dissertation clarified the geometric relation between a lattice and its dual lattice, often overlooked in the literature. Capitalising on that relation, a technique was devised in Chapter 3 that samples points lying on sets of hyperplanes that have the highest density of lattice points on them. Those samples are then quantised to the lattice via zero forcing and the best candidate is declared. The technique exhibits a considerable gain (up to 7 dB in the 4×4 / 64-QAM case) in comparison to OSIC with ZF.

In Chapter 4 it was shown that, whenever exhaustive search is still affordable, it is possible to reduce the number of computations by quantising the whole problem. In doing this, it becomes possible using a lookup-table technique that eliminates many of intermediate operations involved in computing Euclidean distances while still outperforming the traditional receivers.

Many of the now most widely adopted techniques to deal with the CVP were first discovered in the fields of algorithmic number theory. Some authors have conjectured that the Hermite normal form could greatly reduce the number of operations in tree-exploration-based techniques. From the algorithmic point of view, the HNF is not presented in sufficient clarity in the literature. In Chapter 5 an algorithm was given for the HNF and some conclusions drawn regarding the numerical problems that the HNF faces when dealing with random rational lattices. The problems prevent the application of the HNF beyond 4×4 *real* lattices (i.e., 2×2 antennas only). In the same chapter a technique was presented that permits the approximation of a random lattice by one with having one cycle, with a very sparse and triangular generator matrix. However, the numerical problems caused by the very nature of the HNF are directly related with the difficulty of representing the Gaussian lattices of MIMO with a one with one cycle, also defined by a single modular equation.

Chapter 6 derived the property that makes a lattice a member of the family of lattices with a trellis structure and an algorithm was given to create one of those lattices "nearby" the typical Gaussian lattices in MIMO. The basis vectors of the

synthetic lattice and the basis vectors of the original lattice are close and for finite alphabets the two lattices are roughly the same in the region of interest. Given this geometric similarity, the Voronoi regions of both lattices chiefly overlap. A linear transformation then focuses the original lattice onto the synthetic one, known to have a trellis representation. This minimizes the distortion of the Voronoi regions associated with maximum-likelihood detection and therefore the performance attained in the MIMO-CVP is close to optimal.

The distortion between the two lattices is closed by a liner transformation that generalises the concept of zero-forcing. For 2×2, 3×3, 4×4 and 6×6 configurations, decoding on the synthetic lattice outperforms all sub-optimal techniques with or without pre-processing and attains the same diversity as MLD. As expected, the number of cosets necessary for near-optimum performance increases with the dimension of the lattices, just as does the complexity of sphere decoding. However, while the number of nodes to explore in traditional SD is random and dependent on both the lattice and on the received vector itself [186], decoding in a trellis has fixed-complexity during the time that a particular lattice represents the channel.

The last chapter delved into closed loop SM. Using the $\mathrm{LDL}^{\mathrm{T}}$ decomposition, an architecture was proposed that removes complexity from the receiver to the transmitter (often a BS), where it may be more affordable. Additionally, the number of elements required in the feedback channel is about half the one of traditional SVD.

8.2 — Further Work

Lattices continue playing a central role in state-of-the-art research in communication theory. Additionally, because so many problems can be expressed in the language of lattices, techniques to solve open problems in lattice theory always bear a potentially large impact. The following subsections provide a list of open questions bridging some new theories and old problems with aspects of the research presented in this thesis.

8.2.1 — Randomised Projections

As noted at the end of Chapter 3, sampling candidate points near the target vector led to a receiver with a reasonable number of candidates from which to select the best candidate via an exhaustive search. The planes onto which the received point is projected are defined by the dual lattice and therefore, for a given lattice, the planes are deterministic. On the other hand, it has been found very recently that a randomised version of an OSIC-like algorithm achieves full diversity at little complexity, even for large MIMO configurations [232]. The idea is that at each SIC iteration, quantization to the nearest hyperplanes (as in the Babai algorithm) is substituted by a randomised choice [25] of the hyperplane. Several candidates are generated this way by running this randomised SIC several times (the Babai point is forced to be included in the final list of candidates). The idea is then to sample lattice points that, with high probability, are close to the target point, and then select the closest among them. Recently, since the breakthroughs in compressed sampling (CS) [233], [234][26], the study of projections of signals onto random subspaces has become a prominent research topic in signal processing. The concept can also be adapted to assist in the nearest neighbour problem, even if there is not a lattice structure in the point set [235]. It is then natural to ask for a theoretical framework to understand why random projection methods work so well and if they can be put in the context of compressed sampling methods (even though CVP is inherently a l_2-norm problem and CS uses l_1-norm to process sparse data)

[25] The underlying idea is the application of Klein's algorithm, proposed in 2000. Interestingly, the existence of this algorithm had already been noticed by Agrell et al. in the seminal paper [106].

[26] Both papers received *ex aequo* the IEEE Information Theory Paper Award in 2008. An introduction to the topic of CS can be found in[245]. The field is also sometimes called compressed sensing.

8.2.2 — The Orthogonal Sublattice Problem

As seen in 0, the problem of finding a lattice with a trellis structure is equivalent to searching for an orthogonal sublattice for which no research exists in the literature, probably due to the lack of an application. Moreover, one is also interested in finding a sublattice with the smallest possible index (i.e., number of cosets). Finding the best sublattice in polynomial time would make the hierarchy of complexity classes collapse. Indeed, it is not difficult to show that it encompasses the lattice distinguishing problem (LDP), which itself is believed to be NP-hard [224],[106]. A rotated version of a lattice with a very lower number of cosets should lead to the discovery of that same partition. However, as it is not known that if the lattices are the same up to rotation and unimodular transformation, consequently, finding that partition becomes algorithmically unbearable. Nonetheless, devising faster and non-greedy algorithms to replace the one in 0 must be a research objective. One line of possible starting point should be the LLL algorithm which could be relaxed to finding lattice vectors that are orthogonal to all the others but which are not forced to still constitute a basis. In other words, the right-side matrix $\mathbf{M}$ should remain integer but not necessarily unimodular; its determinant should be relaxed to the integer domain instead of being restricted to $\det(\mathbf{M}) \pm 1$. The change of determinant corresponds to a finding sublattice with a certain index.

One other research path should be to find tools for the lattice distinguishing problem itself.

8.2.3 — The Lattice Distinguishing Problem

A promising approach to the LDP is to limit the problem to a finite set of points, instead of considering the infinite lattice. This would involve applying a sphere decoder (similar to the one used in Chapter 3) to capture the points in a certain spherical vicinity of the origin. By doing this, the problem becomes equivalent to the matching point clouds problem (MPCP). If only rotations are considered, then the problem becomes the traditional Procrustes problem [236], [142], [143]. However, as in general a

unimodular transformation of the basis exists simultaneously with the rotation, the problem is a two-sided Procrustes problem, where the right multiplication is a permutation matrix that rearranges the order of the points. Although this is also an open problem, it is simpler than dealing with the infinite lattice. Moreover, MPC is a problem where some research exists given that the problem arises in many applications (medical imaging, robotics, and others). An important contribution to this problem appeared in[237], where the author proposed a technique that iteratively minimizes the rotation (via the well-known Procrustes solution) and permutation matrices (using the Hungarian algorithm [27] [225]). Unfortunately this flip-flop approach almost never converges to a global minimum (i.e., finding the *correct* rotation and the *correct* permutation matrices). If a good method is found to the MPCP, then the lattice distinguishing problem can be solved within the limits of the numerical precision of the cloud of points, but, if needed, more points, with larger distances from the origin, can be added to the set to increase numerical precision.

8.2.4 — Trellis Construction Methods

The research presented in Chapter 6 concerned the *existence* of lattices in $\mathcal{L}_{\mathrm{R}}$ sufficiently close to a given MIMO lattice. Those lattices do have a trellis, though, their explicit *construction* was not given. The obstacle is the practical impossibility of using the HNF that greatly simplifies the projections onto lower dimensional spaces. Therefore, the traditional construction of a trellis as done in [214], [6], [135], [216], [219], [221], is not possible. Devising an efficient method to generate the trellis of a rational lattice, when the lattice is known to have one, is perhaps the most important open question in this thesis.

[27] The Hungarian algorithm solves the *assignment problem*, i.e., finds the optimal assignment between the elements of two sets by minimising the sums of all assignment costs between the elements in the first set and the elements in the second set. The algorithm is also known as the Munkres algorithm.

8.2.5 — Interference Alignment over Lattices

This thesis only considered the case of SM with one Tx and one Rx. In a network environment, in addition to noise and intra-user interference, the receiver is also affected by interference from other users. In a recent theoretical development, Cadambe and Jafar[28] [238], [239] pioneered the idea of interference alignment (IA) in multiuser systems. In MIMO, IA lends itself to the lattice perspective [240] and using specific subspaces to separate users, considering the system as an "expanded" lattice in more dimensions than just $N_R \times N_T$. Assessing the performance of IA methods for different types of MIMO detection algorithms is a research task of high practical importance.

8.2.6 — Physical Layer Network Coding

Physical layer network (PLNC) coding for wireless channels has emerged recently a new way of distributing information between the nodes of a network using fewer physical resources (i.e., channel resources). Lattices also play a key role in these ideas; a prominent approach is based on the properties of nested lattices, as in the pioneering work by Nazer and Gastpar [130], [241], while other approaches to PLNC take advantage of the lattice group property [131]. The structure of the nested lattices greatly simplifies the search for an orthogonal sublattice in them, and therefore they are candidates to have a simple trellis structure. Research in PLNC is very recent and is just in its infancy and most work is still focused on the information theoretical aspects. Mapping nested lattices onto a trellis representation may be an important step for practical implementation of PLNC.

[28] The paper received the IEEE Information Theory Paper Award in 2009. The second reference is a simpler explanation of the key ideas in interference alignment.

Appendix A– Determinant of a Triangular Matrix

This property is used in several chapters of the dissertation.

Theorem: The determinant of a triangular matrix $\mathbf{T}$ corresponds to the product of the elements in the diagonal.

Proof: Consider an upper triangular matrix

$$\mathbf{T} = \begin{bmatrix} t_{11} & t_{12} & & t_{1n} \\ & t_{22} & \cdots & t_{2n} \\ & & \ddots & \vdots \\ & & & t_{nn} \end{bmatrix}. \tag{A.1}$$

By definition, using the cofactors of the matrix and its minors $M_{i,j}$ the determinant is

$$\det(\mathbf{T}) = \sum_{i(\text{or j})=1}^{n} (-1)^{i+j} t_{ij} M_{i,j} = t_{11} \det \begin{pmatrix} t_{22} & \cdots & t_{1n} \\ 0 & \ddots & \\ 0 & 0 & t_{nn} \end{pmatrix}. \tag{A.2}$$

By induction, one gets at the end the product $\det(\mathbf{T}) = \prod_{i=1}^{n} t_{ii}$. A similar procedure also proves the theorem for the case of lower triangular matrixes. ■

Appendix B–
Lattice Geometry Tool

This annex shows the graphical interface (Figure B.1) of a software tool developed in MATLAB® whose aim was to assist the research shown in Chapter 6.

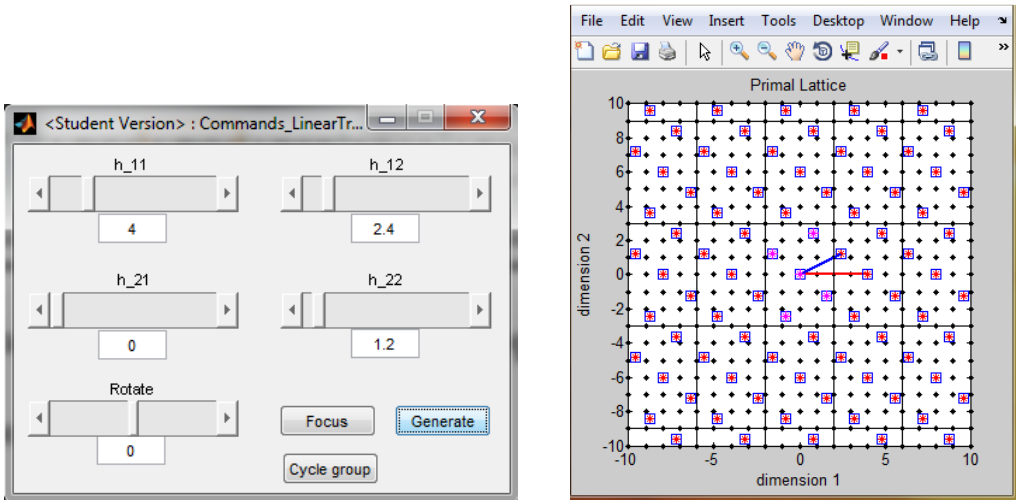


Figure B.1: Command window and generated lattice with a coset partitioning.

References

[1] Claude Shannon, "A mathematical theory of communication," *Bell System Technical*, vol. 27, pp. 379-423, 623-656, July, October 1948.

[2] Neil J. A. Sloane and Aaron D. Wyner, Eds., *Claude E. Shannon: Collected Papers*. New Jersey, USA: IEEE Press, 1993.

[3] Simone Santini, "We are sorry to inform you," *IEEE Computer Magazine*, vol. 38, no. 12, pp. 128, 126-127, December 2005.

[4] Bernard Sklar, "How I learned to love the trellis," *IEEE Signal Processing Magazine,* vol. 20, no. 3, pp. 87 - 102, May 2003.

[5] David G. Forney and Mitchell D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," *IEEE Transactions on Information Theory*, vol. 39, no. 9, pp. 1491-1513, September 1993.

[6] Frank Kschischang and Vladislav Sorokine, "On the trellis structure of block codes," *IEEE Transactionson Information Theory*, vol. 41, no. 6, pp. 1924-1937, November 1995.

[7] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284-287, March 1974.

[8] Ezio Biglieri, "Trellis representation of codes," in *Coding for Wireless Channels*. New York, New York: Springer, 2005, ch. 5, pp. 125-154.

[9] Shu Lin, Tadao Kasami, Toru Fujiwara, and Marc Fossorier, *Trellises and Trellis-based Decoding Algorithms for Linear Block Codes*. Berlin, Germany: Springer, 1998.

[10] Bahram Honary and Garik Markarian, *Trellis Decoding of Block Codes: A Practical Approach*. Berlin, Germany: Springer, 1997.

[11] Daniel J. Costello and G. David Forney, "Channel coding: the road to capacity," *Proceedings of the IEEE*, vol. 95, no. 6, pp. 1150-1177, June 2007.

[12] Francisco Monteiro, "Faster and faster: a look at the remarkable achievements in error-free digital communications," *BlueSci*, no. 15, pp. 14-15, April 2009.

[13] Frank R. Kschischang, "Codes Defined on Graphs," *IEEE Communications Magazine*, vol. 41, no. 8, pp. 118-125, August 2003.

[14] Robert J. McEliece, David J. C. MacKay, and Jung-Fu Cheng, "Turbo decoding as an instance of Pearl's belief propagation," *Journal on Selected Areas on Communications*, vol. 16, no. 2, pp. 140-151, February 1998.

[15] David J. C. MacKay, *Information Theory, Inference and Learning Algorithms*, 3rd ed. Cambridge, UK: Cambridge University Press, 2005.

[16] Henk Wymeersch, *Iterative Receiver Design*. Cambridge, UK: Cambridge University Press, 2007.

[17] David G. Forney, Robert G. Gallager, Gordon R. Lang, Fred M. Longstaff, and Shahid U. Qureshi, "Efficient modulation for band-limited channels," *IEEE Selected Areas in Communications*, vol. SAC-2, no. 5, pp. 632-647, September 1984.

[18] Sergio Benedetto and Ezio Biglieri, "Multidimensional signal constellations: Lattices," in *Principles of Digital Transmission: with Wireless Applications*. New York, New York, USA: Kluwer Academic - Plenum Publishers, 1999, ch. 5.6, pp. 242-252.

[19] Tomaso Aste and Denis Weaire, "Packings and kisses in high dimensions," in *The Persuit of the Perfect Packing*. Bristol, UK: Institute of Physics Publishing, 2000, ch. 12, pp. 113-118.

[20] John H. Conway and Neil J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, New York, USA: Springer, 1999.

[21] G. David Forney and Gottfried Ungerboeck, "Modulation and coding for linear Gaussian channels," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2384-2414, October 1998.

[22] J.A. Sheppard and Alister G. Burr, "A study of performance and decoding complexity in lattice codes," in *Proc. of ISIT'97 - Inter. Symp. on Information Theory*, Ulm, Germany, 1997, p. 523.

[23] Christian Schlegel and Lance Perez, *Trellis and Turbo Coding*. Piscataway, New Jersey, USA: Wiley Interscience - IEEE Press, 2004.

[24] Joseph Boutros, Emanuele Viterbo, Catherine Rastello, and Jean-Claude Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 502-518, March 1996.

[25] Uri Erez and Ram Zamir, "Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293-2314, October 2004.

[26] Naftali Sommer and Meier Feder, "Low-density lattice codes," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1561-1585, April 2008.

[27] David Gesbert, "Breaking the barriers of Shannon's capacity: an overview of MIMO wireless systems," *Telenor's Journal: Telektronikk*, vol. 98, pp. 53-64, January 2002.

[28] Gerard J. Foschini, "Layered space-time architecture for wireless communication in a

fading environment when using multi-element antennas," *Bell labs technical journal*, pp. 41-59, Autumn 1996.

[29] Ì Emre Telatar, "Capacity of multiple-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585-595, November-December 1999.

[30] Arogyaswami Paulraj, Rohit Nabar, and Dhananjay Gore, *Introduction to Space-Time Wireless Communications*. Cambridge, Cambridge: Cambridge University Press, 2003.

[31] Alain Sibille, Claude Oestges, and Alberto Zanella, Eds., *MIMO: From Theory to Implementation*. Amsterdam, Netherlands: Academic Press, 2011.

[32] Erik G. Larsson and Petre Stoica, *Space-Time Block Coding for Wireless Communications*. Cambridge, UK: Cambridge University Press, 2003.

[33] Branka Vucetic and Jinhong Yuan, *Space-Time Coding*. Chichester, UK: Wiley, 2003.

[34] Sergio Barbarossa, *Multiantenna Wireless Communication Systems*, Artech House, Ed. Norwood, Massachusetts, USA: Artech House, 2004.

[35] Ezio Biglieri and Giorgio Taricco, *Transmission and Reception with Multiple Antennas: Theorectical Foundations*. Hanover, Massachusetts, USA: now Publishers, 2004.

[36] Hamid Jafarkhani, *Space-Time Coding - Theory and Practice*. Cambridge, UK: Cambridge University Press, 2005, ch. 9, pp. 221-234.

[37] A. B. Gershman and N. D. Sidiropoulos, *Space-Time Processing for MIMO Communications*. Chischester, UK: John Wiley & Sons, 2005.

[38] Helmut Bölcskei, David Gesbert, Constantinos B. Papadias, and Alle-Jan van der Veen, *Space-Time Wireless Systems - From Array Processing to MIMO Communications*. Cambridge, UK: Cambridge Universty Press, 2006.

[39] Volker Kühn, *Wireless Communications over MIMO Channels - Applications to CDMA and Multiple Antenna Systems*. Chischester, UK: Wiley, 2006.

[40] Ezio Biglieri et al., *MIMO Wireless Communications*. Cambridge, UK: Cambridge University Press, 2007.

[41] Georgios Giannakis, Zhiqiang Liu, Xiaoli Ma, and Shengli Zhou, *Space-Time Coding for Broadband Wireless Communications*. Hoboken, New Jersey, USA: Wiley, 2007.

[42] Tolga M. Duman and Ali Ghrayeb, *Coding for MIMO Communication Systems*. Chischester, UK: John Wiley & Sons, 2007.

[43] Claude Oestges and Bruno Clerckx, *MIMO Wireless Communications: From Real-World Propagation to Space-Time Code Design*. Oxford, UK: Academic Press / Elsevier, 2007.

[44] Andrea Goldsmith, *Wireless Communications*. Cambridge, UK: Cambridge University Press, 2005.

[45] David Tse and Pramod Viswanath, *Fundamentals of Wireless Communication*. Cambridge, UK: Cambridge University Press, 2005.

[46] Behrouz Farhang-Boroujeny, "OFDM Versus Filter Bank Multicarrier," *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 92-112, May 2011.

[47] Hongwei Yang, "A road to future broadband wireless access: MIMO-OFDM-Based air interface," *IEEE Communications Magazine*, vol. 43, no. 1, pp. 53-60, January 2005.

[48] Wei Zhang, Xia Xiang-Gen, and Khaled Ben Letaief, "Space-Time/Frequency Coding for MIMO-OFDM in Next Generation Broadband Wireless Systems," *IEEE Wireless Communications*, vol. 14, no. 3, pp. 32-43, June 2007.

[49] Qinghua Li et al., "MIMO techniques in WiMAX and LTE: a feature overview," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 86-92, May 2010.

[50] Jeffrey G. Andrews, Arunabha Ghosh, and Rias Muhamed, *Fundamentals of WiMAX*. Upper Saddle River, New Jersey, USA: Prentice Hall - Pearson Education, 2007.

[51] Farooq Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge, UK: Cambridge University Press, 2009.

[52] Stefania Sesia, Mr Matthew Baker, and Mr Issam Toufik, Eds., *LTE - the UMTS long term evolution: from theory to practice*. Chichester, UK: John Wiley & Sons, 2009.

[53] Arunabha Ghosh, Jun Zhang, Jeffrey G. Andrews, and Rias Muhamed, *Fundamentals of LTE*. Boston, Massachusetts, USA: Prentice Hall, 2010.

[54] Quentin H. Spencer, Christian B. Peel, A. Lee Swindlehurst, and Martin Haardt, "An introduction to the multi-user MIMO downlink," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 60-67, October 2004.

[55] Amitava Ghosh, Rapeepat Ratasuk, Bishwarup Mondal, Nintin Mangalvedhe, and Tim Thomas, "LTE-advanced: next-generation wireless broadband technology," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 10-22, June 2010.

[56] Chester Sungchung Park, Y.-P. Eric Wang, George Jöngren, and David Hammarwall, "Evolution of uplink MIMO for LTE-advanced," *IEEE Communications Magazine*, vol. 49, no. 2, pp. 112-121, February 2011.

[57] Dongwoon Bai, Hoang Nguyen, Taeyoon Kim, and Inyup Kang, "LTE-Advanced modem design: challenges and perspectives," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 178-186, February 2012.

[58] Stefan Parkvall, Anders Furuskär, and Erik Dahlman, "Evolution of LTE toward IMT-advanced," *IEEE Communications Magazine*, vol. 49, no. 2, pp. 84-91, February 2011.

[59] Sassan Ahmadi, "An overview of next-generation mobile WiMAX technology," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 84-98, June 2009.

[60] Per Ödling, Thomas Magesacher, Per Ola Börjesson Stefan öst, Miguel Berg, and Enrique Areizaga, "The fourth generation broadband concept," *IEEE Communications Magazine*, vol. 43, no. 1, pp. 63-69, January 2009.

[61] Qinghua Li, Xintian Eddie Lin, Jianzhong (Charlie) Zhang, and Wonil Roh, "Advancement

of MIMO technology in WiMAX: from IEEE 802.16d/e/j to 802.16m," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 100-107, June 2009.

[62] Yan Zhang and Hsiao-Hwa Chen, *Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks*. Boca Raton, Florida, USA: Auerbach Publications, 2008.

[63] Krystian Safjan et al., "Assessing 3GPP LTE-advanced as IMT-advanced technology: the WINNER+ evaluation group approach," *IEEE Communications Magazine*, vol. 49, no. 2, pp. 92-100, February 2011.

[64] Eldad Perahia and Robert Stacey, *Next Generation Wireless LANs - Throughput, Robustness, and Reliability in 802.11n*. Cambridge, UK: Cambridge University Press, 2008.

[65] Guido R. Hiertz et al., "The IEEE 802.11 universe," *IEEE Communications Magazine*, vol. 48, no. 1, pp. 62-70, January 2010.

[66] Tuncer Baykas et al., "IEEE 802.15.3c: the first IEEE wireless standard for data rates over 1 Gb/s," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 114-121, July 2011.

[67] Richard Van Nee, "Breaking the gigabit-per-second barrier with 802.11ac," *IEEE Wireless Communications*, vol. 18, no. 2, p. 4, April 2011.

[68] Arogyaswami J. Paulraj, Dhananjay A. Gore, Rohit U. Nabar, and Helmut Bölcskei, "An overview of MIMO communications - a key to gigabit wireless," *Proceedings of the IEEE*, vol. 92, no. 2, pp. 198-218, February 2004.

[69] Howard R. Stuart, "Dispersive Multiplexing in Multimode Optical Fiber," *Science*, vol. 289, pp. 281-283, July 2000.

[70] Fernando Pérez-Cruz, Miguel R. Rodrigues, and Sergio Verdú, "Optimal precoding for digital subscriber lines," in *Proc. of ICC'08 - The IEEE Inter. Conf. on Communications*, Beijing, May 2008, pp. 1200-1204.

[71] L. H. Brandenburg and A. D. Wyner, "Capacity of the Gaussian Channel with Memory: The Multivariate Case," *Bell Systems Technical Journal*, vol. 53, no. 5, pp. 745–778, May 1974.

[72] Lizhong Zheng and David N.C. Tse, "Diversity and multiplexing:a Fundamental tradeoff in multiple antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.

[73] Siavash M. Alamouti, "A simple transmit diversity for technique wireless communications," *IEEE Journal on Selected Areas on Communications*, vol. 16, no. 8, pp. 1451-1458, October 1998.

[74] Vahid Tarokh, Hamid Jafarkhani, and A. Robert Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1456-1467, July 1999.

[75] Ender Ayanoglu, Erik G. Larsson, and Eleftherios Karipidis, "Computational complexity of decoding orthogonal space-time block codes," *IEEE Transactions on Communications*, vol.

59, no. 4, pp. 936-941, April 2011.

[76] Vahid Tarokh, Nambi Seshadri, and A. Robert Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744-765, March 1998.

[77] Emanuele Viterbo and Frédérique Oggier, *Algebraic Number Theory and Code Design for Rayleigh Fadign Channels*. Hanover, Massachusetts, USA: now Publishers, 2004.

[78] Frédérique Oggier, Ghaya Rekaya, Jean-Claude Belfiore, and Emanuele Viterbo, "Perfect space-time block codes," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 3885-3902, September 2006.

[79] Frédérique Oggier, "Algebraic methods for channel coding," PhD Thesis, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2005.

[80] Hesham El Gamal, Giuseppe Caire, and Mohamed Oussama Damen, "Lattice coding and decoding achieve the optimal diversity–multiplexing tradeoff of MIMO channels," *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 968-985, June 2004.

[81] Karen Su, Inaki Berenguer, Ian J. Wassell, and Xiaodong Wang, "Efficient maximum-likelihood decoding of spherical lattice codes," *IEEE Transactions on Communications*, vol. 57, no. 8, pp. 2290-2300, August 2009.

[82] Maurizio Magarini, "Spatial loading in V-BLAST systems with limited feedback and ZF-OSIC detection," in *Proc. of the 4th Inter. Symp. on Wireless Communication Systems (ISWCS)*, Trondheim, Norway, 2007, pp. 350-354.

[83] Bertrand M. Hochwald and Stephan ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 389-399, March 2003.

[84] Yi Jiang, Mahesh K. Varanasi, and Jian Li, "Performance analysis of ZF and MMSE equalizers for MIMO systems: an in-depth study of the high SNR regime," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2008-2026, April 2011.

[85] G. D. Golden, C. J. Foschini, R. A. Valenzuela, and P. W. Wolniansky, "Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture," *IET Electronics Letters*, vol. 35, no. 1, January 1999.

[86] Wai Ho Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," MPhil Thesis, Chinese University of Hong Kong, Hong Kong, Hong Kong, 1991.

[87] Sergio Verdú, *Multiuser Detection*. Cambridge, UK: Cambridge University Press, 1998.

[88] Wei Zhang, Xiaoli Ma, B. Gestner, and D. Anderson, "Designing low-complexity equalizers for wireless systems," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 56-62, January 2009.

[89] Kenichi Kobayashi, Tomoaki Ohtsuki, and Toshinobu Kaneko, "MIMO systems in the presence of feedback delay," *IEICE Transactions on Communications*, vol. E91-B, no. 3,

pp. 829-836, March 2008.

[90] Mai Vu and Arogyaswami Paulraj, "MIMO wireless linear precoding," *IEEE Signal Processing Magazine*, vol. 24, no. 5, pp. 86-105, September 2007.

[91] Mohammed El-Hajjar and Lajos Hanzo, "Multifunctional MIMO systems: A combined diversity and multiplexing design perspective," *IEEE Wireless Communications*, vol. 17, no. 2, pp. 73-79, April 2010.

[92] Robert W. Heath and Arogyaswami J. Paulraj, "Switching between diversity and multiplexing in MIMO systems," *IEEE Transactions on Communications*, vol. 53, no. 6, pp. 962-968, June 2005.

[93] A. Lozano and N. Jindal, "Transmit diversity vs. spatial multiplexing in modern MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 186 - 197, January 2010.

[94] Robert F. H. Fischer, *Precoding and Signal Shaping for Digital Transmission*. Chischester, UK: John Wiley & Sons, 2005.

[95] Christoph Windpassinger, "Detection and precoding for multiple input multiple output channels," PhD thesis, University of Erlangen-Nürnberg, Erlangen, Germany, 2004.

[96] Mahmoud Taherzadeh, "Lattice-based precoding and decoding in MIMO fading systems," PhD thesis, University of Waterloo, Waterloo, Ontario, Canada, 2008.

[97] Andrea Goldsmith, Syed Ali Jafar, and Nihar Jindal, "Capacity limits of MIMO channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 5, pp. 684-701, June 2003.

[98] Hanan Weingarten, Yossef Steinberg, and Shlomo Shamai (Shitz), "The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channel," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 3936-3964, September 2006.

[99] David J. Love, Robert W. Heath, Wiroonsak Santipach, and Michael L. Honig, "What is the value of limited feedback for MIMO channels," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 54-59, October 2004.

[100] Laude Simon and Geert Leus, "Feedback quantization for linear precoded spatial multiplexing," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, January 2008.

[101] Rick S. Blum, "MIMO with limited feedback of channel state information," in *Proc. of IEEE Inter. Conf. Acoustics, Speech, Signal Processing (ICASSP)*, Hong-Kong, China, April 2003, pp. IV-89-IV-92.

[102] Nihar Jindal, "MIMO broadcast channels with finite-rate feedback," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 5045-5060, 2006 2006.

[103] Hendrik W. Lenstra, "Lattices," in *Algorithmic Number Theory*, J. P. Buhler and P. Stevenhagen, Eds. Cambridge, UK: Cambridge University Press, 2008, pp. 127-181.

[104] "Special issue on complexity reduction in MIMO," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 6, December 2009.

[105] Ram Zamir, "Lattices are everywhere," in *Proc. of the Information Theory and Applications Workshop*, San Diego, California, USA, February 2009, pp. 392-421.

[106] Erik Agrell, Thomas Eriksson, Alexander Vardy, and Kenneth Zeger, "Closest point in lattices," *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2201-2214, August 2002.

[107] Phong Q. Nguyen and Daniele Micciancio, "Entries on Lattice, Shortest Vector Problem, Closest Vector Problem, and Lattice Based Cryptography," in *Encyclopedia of Cryptography and Security*, Henk C. A. van Tilborg, Ed. New York, New York, USA: Springer, 2005, pp. 345-349.

[108] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 2nd ed. Berlin, Germany: Springer, 1971.

[109] Alexandre Schrijver, *Theory of Linear and Integer Programming*. Chischester, UK: John Wiley & Sons, 1986, ch. 4, 5, 6.

[110] László Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*. Philadelphia, Pennsylvania, USA: Society for Industrial and Applied Mathematics (SIAM), 1986, ch. 1, pp. 15-38.

[111] Ravi Kannan, "Algorithmic geometry of numbers," *Annual Review of Computer Science*, vol. 2, pp. 231-267, June 1987.

[112] Dimitris Bertsimas and Robert Weismantel, *Optimization over Integers*. Belmont, MA, USA: Dynamic Ideas, 2005.

[113] Daniele Micciancio and Shafi Goldwasser, *Complexity of Lattice Problems - A Cryptographic Perspective*. Norwell, Massachusetts, USA: Kluwer Academic Publishers, 2002.

[114] Eric Dubois, "The sampling and reconstruction of time-varying imagery with applications in video systems," *Proceedings of the IEEE*, vol. 73, no. 4, pp. 502-522, April 1985.

[115] Ran Zamir, "On lattice quantization noise," *Transactions on Information Theory*, vol. 42, no. 4, pp. 1152-1159, July 1996.

[116] Erik Agrell and Thomas Eriksson, "Optimization of lattices for quantization," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1814-1828, September 1998.

[117] G. David Forney, "Coset codes - Part I: introduction and geometrical classification," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1123-1151, September 1988.

[118] Mahmoud Taherzadeh, Amin Mobasher, and Amir K. Khandani, "Communication over MIMO broadcast channels using lattice-basis reduction," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4567-4582, December 2007.

[119] Erik G. Larsson, "MIMO detection methods: how they work," *IEEE Signal Processing*

Magazine, vol. 26, no. 3, pp. 91-95, May 2009.

[120] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST: an architecture for realizing very high data rates over the rich-scattering wireless channel," in *Proc. of URSI Int. Symposium on*, Pisa, Italy, September 1998, pp. 295-300.

[121] Wai Ho Mow, "Universal lattice decoding: principles and recent advances," *Wireless Communications and Mobile Computing*, vol. 3, pp. 553-569, March 2003.

[122] Steven Galbraith, *Mathematics of Public Key Chryptography*. Cambridge, UK: Cambridge University Press (commissioned), to be published, ch. 18,19,20,22.

[123] Emanuele Viterbo and Joseph Boutros, "A universal lattice code decoder for fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1639-1642, July 1999.

[124] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, no. 170, pp. 463-471, April 1985, Was unable to find their first names.

[125] C. P. Schnorr and M. Euchner, "Lattice basis reduction: improved practical algorithms and solving subset sum problems," *Mathematical Programming*, vol. 66, pp. 191-199, 1994.

[126] Huan Yao and G.W. Wornell, "Lattice-reduction-aided detectors for MIMO communication systems," in *Proc. of GLOBECOM' 02 - IEEE Global Telecommunications Conference*, Taipei, Taiwan, 2002, pp. 424 -428.

[127] Dominik Seethaler, Gerald Matz, and Franz Hlawatsch, "Low-Complexity MIMO Data Detection using Seysen's Lattice Reduction Algorithm," in *Proc. of ICASSP'07 - IEEE Inter. Conf. on Acoustics, Speech and Signal Processing*, Honolulu, Hawaii, USA, April 2007, pp. 15-20.

[128] Jun Niu and I-Tai Lu, "A new lattice-reduction-based receiver for MIMO systems," in *Proc. of CISS - 41st Annual Conf. on Information Sciences and Systems*, Baltimore, Mariland, March 2007, pp. 499-504.

[129] Phong Q. Nguyen and Brigitte Vallée, Eds., *The LLL Algorithm*. Berlin, Germany: Springer, 2010.

[130] Bobak Nazer and Michael Gastpar, "Reliable physical layer network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438-460, March 2011.

[131] Chen Feng, Danilo Silva, and Frank R. Kschischang, "An algebraic approach to physical-layer network coding," in *Proc. of ISIT'10 - The Inter. Symp. on Information Theory*, Austin, TX, USA, June 2010, pp. 1017-1021.

[132] Daniele Micciancio and Oded Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, Eds. Berlin, Germany: Springer, 2009, pp. 146-191.

[133] Norman L. Biggs, *Discrete Mathematics*. Oxford, UK: Oxford University Press, 2002.

[134] Carl Ludwig Siegel, *Lectures on the Geometry of Numbers*. Berlin, Germany: Springer, 1989.

[135] Amir H. Banihashemi, "Decoding complexity and trellis structure of lattices," PhD thesis, University of Waterloo, Waterloo, Ontario, Canada, 1997.

[136] A. Paz and C. P. Schnorr, "Approximating integer lattices by lattices with cycle factor groups," in *Proc. of the 14th Inter. Conf. on Automata, Languages and Programming*, Karlsruhe, Germany, LNCS 267, July 1987, pp. 386-393.

[137] Mårten Trolin, "Lattices with Many Cycles Are Dense," in *Proc. of the 21th Inter. Conference on Theoretical Aspects of Computer Science (STACS)*, Montpllier, France, LNCS 2996, March 2004, pp. 370-381.

[138] Ian H. Sloan and Stephen Joe, *Lattice Methods for Multiple Integration*. Oxford, UK: Oxford University Press, 1994.

[139] Carl D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Philadelphia, Pennsylvania : Society for Industrial and Applied Mathematics (SIAM), 2000.

[140] Alan Edelman, Tomás A. Arias, and Steven T. Smith, "The geometry of algorithms with orthogonality constraints," *SIAM Journal on Matrix Analysis and Applications (SIMAX)*, vol. 20, no. 2, pp. 303-353, July 1998.

[141] Utpal Banerjee, "Unimodular Matrices," in *Loop Transforms for Restructuring Compilers*. Dordrecht, The Netherlands: Kluwer Academic Press, 1993, ch. 2.

[142] John C. Gower, "Procrustes methods," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, pp. 503-508, July/August 2010.

[143] John C. Gower and Garmt B. Dijksterhuis, *Procrustes Problems*. Oxford, UK: Oxford University Press, 2004.

[144] Nicholas H. Higham, "Matrix nearness problems and applications," in *Applications of Matrix Theory*, M. J. C. Gover and S. Barnett, Eds. Oxford, UK: Oxford University Press, 1989, pp. 1-27.

[145] Cong Ling, Lu Gan, and Wai Ho Mow, "A dual-lattice view of V-BLAST detection," in *Proc. of ITW' 06, The IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 478-482.

[146] Cong Ling and Wai Ho Mow, "A unified view of sorting in lattice reduction: From V-BLAST to LLL and beyond," in *Proc. of the IEEE Inform. Theory Workshop*, Taormina, Italy, 2009, pp. 529-533.

[147] Karen Su and Frank R. Kschischang, "Coset-based lattice detection for MIMO systems," in *Proc. of ISIT'07 - IEEE Inter. Symp. on Information Theory*, Nice, France, June 2007, pp. 1941 - 1945.

[148] G. W. Stewart, *Introduction to Matrix Computations*. London, UK: Academic Press, 1973.

[149] Antonia M. Tulino and Sergio Verdú, *Random Matrix Theory and Wireless*

Communications. Delft, Netherlands: Now, 2004, ch. 2, pp. 24-38.

[150] Petre Stoica, Yi Jiang, and Jian Li, "On MIMO channel capacity: an intuitive discussion," *IEEE Signal Processing Magazine*, vol. 22, no. 3, pp. 83-84, May 2005.

[151] Dorit S. Hochba, Ed., *Approximation Algorithms for NP-Hard Problems*. Boston, Massachusetts , USA: Course Technology / PWS Publishing Company, 1996.

[152] Christopher M. Bishop, "The curse of dimensionality," in *Pattern Recognition and Machine Learning*. New York, NY: Springer, 2006, ch. 1.4, pp. 33-38.

[153] John Talbot and Dominic Welsh, *Complexity and Cryptography: an Introduction*. Cambridge, UK: Cambridge University Press, 2006.

[154] Dominic Welsh, "Computational Complexity," in *Codes and Cryptography*. Oxford, UK: Oxford University Press, 1988, ch. 9, pp. 143-148.

[155] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein, "NP-completeness," in *Introduction to Algorithms*, 2nd ed. Cambridge, Massachusetts, USA: MIT Press, 2001, ch. 34.

[156] Donald L. Kreher and Douglas R. Stinson, *Combinatorial Algorithms: Generation, Enumeration, and Search*. Boca Raton, Florida, USA: CRC Press, 1999.

[157] Daniele Micciancio, "The hardness of the shortest vector problem with preprocessing," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1212-1215, March 2001.

[158] Robert Piziak and P. L. Odell, *Matrix Theory - From Generalized Inverses to Jordan Form*. Boca Raton, Florida, USA: Chapman & Hall - CRC, 2007.

[159] Joan Westlake, *Handbook of Numerical Matrix Inversion and Solution of Linear Equations*. Chischester, UK: John Wiley & Sons, 1968, ch. 2.6.

[160] Cong Ling, "On the proximity factors of lattice reduction-aided decoding," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2795-2808, June 2011.

[161] Xiaoli Ma, Wei Zhang, and Ananthram Swami, "Lattice-reduction aided equalization for OFDM systems," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1608-1613, April 2009.

[162] Simon Haykin, *Adaptive Filter Theory*, 3rd ed. Upper Saddle River, New Jersey, EUA: Prentice Hall, 1996.

[163] Upamanyu Madhow, *Fundamentals of Digital Communication*. Cambridge, UK: Cambridge University Press, 2008.

[164] Steven M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory, Vol. I*. Upper Saddle River, New Jersey, USA: Prentice Hall, 1993.

[165] Babak Hassibi, "An efficient square-root algorithm for BLAST," in *Proc. of ICASSP '00 - IEEE Inter. Conf. on Acoustics, Speech, and Signal Processing*, vol. 2, Istanbul, Turkey, 2000, pp. II737-II740.

[166] Li Hong and Ana Garcia Armada, "Bit error rate performance of MIMO MMSE receivers

in correlated Rayleigh flat-fading channels," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 313-317, January 2011.

[167] Namshik Kim, Yusung Lee, and Hyuncheol Park, "Performance analysis of MIMO system with linear MMSE receiver," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 447-44478, November 2008.

[168] Joakim Jaldén and Björn Ottersten, "High diversity detection using semidefinite relaxation," in *40th Asilomar Conf. on Signals, Systems and Computers*, Pacific Grove, California, USA, 2006, pp. 2082-2086.

[169] Laszlo Babai, "On Lovász' lattice reduction and the nearest lattice," *Combinatoria*, vol. 6, no. 1, pp. 1-13, January 1986.

[170] Yue Shang and Xiang-Gen Xia, "An improved fast recursive algorithm for V-BLAST with optimal ordered detections," in *Proc of ICC'08 - IEEE Inter. Conference on Communications*, Beijing, China, May 2008, pp. 756-760.

[171] Cong Ling, Wai Ho Mow, and Lu Gan, "Dual-lattice ordering and partial lattice reduction for SIC-based MIMO detection," *IEEE Journal in Selected Topics in Signal Processing*, vol. 3, no. 6, pp. 975-985, December 2009.

[172] Rafael A. Trujillo, Victor M. Garcia, Antonio M. Vidal, Sandra Roger, and Alberto Gonzalez, "A gradient-based ordering for MIMO decoding," in *Proc. of the 9th IEEE Inter. Symp. on Signal Processing and Information Technology (ISSPIT)*, Ajman, United Arab Emirates, 2009, pp. 5-8.

[173] Mahmoud Taherzadeh, Amin Mobasher, and Amir K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4801-4805, December 2007.

[174] Huan Yao, "Efficient signal, code and receiver designs for MIMO communications systems," Massachusetts Institute of Technology, Cambridge, Massachusetts, USA, PhD thesis 2003.

[175] Dirk Wübben, Dominik Seethaler, Joakim Jaldén, and Gerald Matz, "Lattice Reduction," *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 70-91, May 2011.

[176] Ying H. Gan, Cong Ling, and Wai Ho Mow, "Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection," *IEEE Transactions in Signal Processing*, vol. 57, no. 7, pp. 2701 - 2710, July 2009.

[177] Robert Fischer, "From Gram–Schmidt orthogonalization via sorting and quantization to lattice reduction," in *Proc. of the 6th Joint Workshop on Coding and Communications (JWCC)*, Santo Stefano Belbo, Italy, 2010, pp. 13-17.

[178] C. Ling and W. H. Mow, "A unified view of sorting in lattice reduction: From V-BLAST to LLL and beyond," in *Proc. of the IEEE Inf. Theory Workshop*, Taormina, Italy, 2009, pp. 529-533.

[179] Jaehyun Park, Joohwan Chun, and Franklin T. Luk, "Lattice reduction aided MMSE

Decision Feedback Equalizers," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 436-441, January 2011.

[180] Cong Ling, Wai Ho Mo, and Nick Howgrave-Graham, "Variants of the LLL algorithm in digital communications: complexity analysis and fixed-complexity implementation," *Submitted to IEEE Transactions on Information Theory, arXiv:1006.1661v2 [cs.IT]*, 2010.

[181] Joakim Jaldén, Dominik Seethaler, and and Gerald Matz, "Worst- and average-case complexity of LLL lattice reduction in MIMO wireless systems," in *Proc. of ICASSP'08 - The IEEE Inter. Conf. on Acoustics, Speech and Signal Processing*, Las Vegas, NV, USA, April 2008, pp. 2685 - 2688.

[182] Sandra Roger, Alberto Gonzalez, Vicenc Almenar, and Antonio M. Vidal,. Limassol, Cyprus, March 2010.

[183] Atsushi Okawado, Ryutaroh Matsumoto, and Tomohiko Uyematsu, "Near ML detection using Dijkstra's algorithm with bounded list size over MIMO channels," in *Proc. of ISIT'08 - IEEE Inter. Symp. on Information Theory*, Toronto, Canada, July 2008, pp. 2022-2025.

[184] Thorben Detert, "An efficient fixed complexity QRD-M Algorithm for MIMO-OFDM using per-survivor slicing," in *Proc. of ISWCS'07, 4th International Symposium on Wireless Communication Systems*, Trondheim, October 2007, pp. 572-576.

[185] Karen Su, "Detection and decoding of signals transmitted over linear MIMO channels," PhD thesis, University of Cambridge, Cambridge, UK, 2005.

[186] Karen Su and Ian J. Wassell, "A new ordering for efficient sphere decoding," in *Proc. of ICC'05 - The IEEE Inter. Conf. on Communications*, vol. 3, Seoul, Korea, 2005, pp. 1906-1910.

[187] Arash Ghasemmehdi and Erik Agrell, "Faster recursions in sphere decoding," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3530-3536, June 2011.

[188] Babak Hassibi and Haris Vikalo, "On the sphere-decoding algorithm I. Expected complexity," *IEEE Transactions on signal Processing*, vol. 53, no. 8, pp. 2806-2818, August 2005.

[189] Joakim Jaldén and Björn Ottersten, "On the complexity of sphere decoding in digital communications," *IEEE Transactions on Signal Processing*, vol. 53, no. 4, pp. 1474-1484, April 2005.

[190] L. G. Barbero and J. S. Thompson, "Fixing the complexity of the sphere decoder for MIMO detection," *Trans. Wireless Commun*, vol. 7, no. 6, pp. 2131-2142, June 2008.

[191] Kuei-Chiang Lai, Cheng-Chieh Huang, and Jiun-Jie Jia, "Variation of the fixed-complexity sphere decoder," *IEEE Communications Letters*, vol. 15, no. 9, pp. 1001-1003, September 2011.

[192] Joakim Jaldén, Luis G. Barbero, Björn Ottersten, and John S. Thompson, "The error probability of the fixed-complexity sphere decoder," *IEEE Transactions on Signal*

Processing, vol. 57, no. 7, pp. 2711-2720, July 2009.

[193] M. C. Jeruchim, Philip Balaban, and K. Sam Shanmugan, *Simulation of Communication Systems: Modelling, Methodology and Techniques.*: Kluwer Academic / Plenum Publishers, 2000, ch. 11.2.3.

[194] Francisco Monteiro, "Complexity reduction of CPM detection in wireless communication systems (in Portuguese)," Masters thesis, Instituto Superior Técnico, Technical University of Lisbon, Portugal, 2003.

[195] Andrew Stothers, "On the complexity of matrix multiplication," PhD thesis, University of Edimburgh, Edimburgh, Scotland, United Kingdom, 2010.

[196] Yoshikazu Ohashi, "Fast linear approximations of Euclidean distances in higher order dimensions," in *Graphics Gems IV*. Morgan Kaufmann, 1994, pp. 120-124.

[197] Mauro Barni, Franco Bartolini, and Vito Cappelini, "A quasi-Euclidean norm to speed up vector median filtering," *IEEE Transactions on Image Processing*, vol. 9, no. 10, pp. 1704-1709, october 2000.

[198] Markus Rupp, Gerhard Gritsch, and Hans Weinrichter, "Approximate ML detection for MIMO systems with very low complexity," in *Proc. of ICASSP' - IEEE Int. Conference on Acoustics, Speech, and Signal Processing*, vol. IV, Montreal, 2004, pp. 809-812.

[199] Syed A. Rizvi and Nasser M. Nasrabadi, "An efficient Euclidean distance computation for vector quantization using a truncated look-up table," *IEEE Transactions on circuits and systems for video technology*, vol. 5, No. 4, pp. 370–371, no. 4, pp. 370-371, August 1995.

[200] C.-C. Chang, J.-S. Chou, and T.-S. Chen, "An efficient computation of Euclidean distances using approximated look-up table," *IEEE Trans. on circuits and systems for video technology*, vol. 10, no. 4, April 2000.

[201] N. Benvenuto and U. Cherubini, *Algorithms for Communications Systems and their Applications*. Chischester, UK: Willey, 2002, ch. 5.

[202] M. Magarini and A. Spalvieri, "Performance evaluation of the V-BLAST coset detector," in *Proc. of ISWCS'05- 2nd Inter. Symposium on Wireless Communication Systems*, September 2005, pp. 18-21.

[203] Maurice V. Wilkes. (2002, October) [Online]. http://www.cl.cam.ac.uk/archive/mvw1/unpublished.html

[204] Arul D. Murugan, Hesham El Gamal, Mohamed Oussama Damen, and Giuseppe Caire, "A unified framework for tree search decoding: rediscovering the sequential decoder," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 933-953, March 2006.

[205] Arul D. M. Palanivelu, "Tree search algorithms for joint detection and decoding," PhD thesis, Ohio State University, Columbus, Ohio, USA, 2006.

[206] Charles C. Sims, *Computation with Finitely Presented Groups*. Cambridge, UK: Cambridge University Press, 1994.

[207] Madhan K. Vairamuthu, "Hermite normal Form: Algorithmic Analysis," Australia, PhD thesis, University of Queensland 2003.

[208] R. Kannan and A. Bachem, "Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix," *SIAM Journal of Computing*, vol. 9, pp. 499-507, 1979.

[209] Rudolf Lidl and Günter Pilz, "Lattices," in *Applied Abstract Algebra*, 2nd ed. New York, New York, USA: Springer, 2nd ed., 2010, ch. 1, pp. 1-53.

[210] A. H. Banihashemi, "Decoding complexity and trellis structure of lattices," PhD thesis, University of Waterloo, Ontario, Canada, 1997.

[211] Vahid Tarokh and Ian F. Blake, "Trellis complexity versus the coding gain of lattices I," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1796-1807, November 1996.

[212] Vahid Tarokh and Alexander Vardy, "Upper bounds on trellis complexity of lattices," *IEEE Transactions on Information Theory*, vol. 42, no. 4, pp. 1294-1300, July 1997.

[213] Carlos Aguilar Melchor, Guilhem Castagnos, and Philippe Gaborit, "Lattice-based homomorphic encryption of vector spaces," in *Proc. of ISIT'08 - IEEE Inter. Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 1858-1862.

[214] G. David Forney, "Coset codes - part II: binary lattices and related codes," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152-1187, September 1988.

[215] A. Robert Calderbank and Neil J. A. Sloane, "New trellis codes based on lattices and cosets," *IEEE Transactions in Information Theory*, vol. IT-33, no. 2, pp. 177-195, March 1987.

[216] Alexander Vardy, "Trellis Structure of Codes," in *Handbook of Coding Theory*, Vera Pless and W. Cary Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 24, pp. 1989-2117.

[217] Alister G. Burr and J. A. Sheppard, "Hardware architectures for lattice decoders," in *Proc. of the IEE Colloquium on DSP Applications in Communication Systems*, London, UK, 1993, pp. 8/1-8/6.

[218] Jin Lee and Sin-Chong Park, "MIMO Detector Based on Trellis," *IEICE Transactions on Communications*, vol. E91-B, no. 3, pp. 951-954, March 2008.

[219] Amir H. Banihashemi and Frank R. Kschischang, "Tanner graphs for group block codes and lattices: construction and complexity," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 822-834, February 2001.

[220] Amir H. Banihashemi and Ian F. Blake, "Trellis complexity and minimal trellis diagrams of lattices," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1829-1845, September 1998.

[221] Haibin Kan and Hong Shen, "The bases associated with trellis of a lattice," *IEICE Transactions on Fundamentals*, vol. E88-A, no. 7, pp. 2030-2033, July 2005.

[222] Daniele Micciancio and Shafi Goldwasser, *Complexity of Lattice Problems - A*

Cryptographic Perspective. Norwell, Massachusetts, USA: Kluwer Academic Publishers, 2002.

[223] Michael Szydlo, "Hypercubic lattice reduction and analysis of GGH and NTRU signatures," in *Proc. of Eurocrypt 2003*, Warsaw, Poland, LNCS 2656, 2003, pp. 433-448.

[224] Khanh Nguyen, "An identification scheme from lattice distinguishing problem," Gemplus R&D, unpublished, available online, Singapore, Singapore,.

[225] Kenneth A. Berman and Jerome L. Paul, "Matching and network flow algorithms," in *Algorithms: Sequantial, Parallel and Distribuited*. Boston, Massachussetts: Thomson, 2005, ch. 14, pp. 418-427.

[226] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2010, ch. 5, p. 230.

[227] G. David Forney, "Density / length profiles and trellis complexity of lattices," *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 1753-1772, November 1994.

[228] M. O. Rabin and J. O. Shallit, "Randomized algorithms in number theory," *Communications on Pure and Applied Mathematics*, vol. 39:Suplement, pp. S239-S256, 1986.

[229] Gene H. Golub and Charles F. Van Loan, *Matrix Computations*, 3rd ed. Baltimore, Maryland, USA: The Hohns Hopkins University Press, 1996.

[230] Che-Chen Chou, Hsi-Chei Chen, and Jen-Ming Wu, "A low complexity channel decomposition and feedback strategy for MIMO precoder design," in *Proc. of ICASSP'09 - The IEEE Inter. Conf. on Acoustics, Speech and Signal Processing*, Taipei, Taiwan, April 2009, pp. 2705-2707.

[231] Giuseppe Caire, "President's Column," *IEEE Information Theory Society Newsletter*, vol. 61, no. 1, pp. 1,3, March 2011.

[232] Shuiyin Liu, Cong Ling, and Damien Stehlé, "Randomized lattice decoding," *IEEE Transations on information Theory*, to appear.

[233] David Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289-1306, April 2006.

[234] Emmanuel Candés and Terence Tao, "Near-optimal signal recovery from random projections: universal encoding strategies?," *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406-5425, December 2006.

[235] Santosh S. Vempala, "Nearest Neighbours," in *The Random Projection Method*. Providence, Rhode Island: American Mathematical Society, 2004, ch. 7.

[236] Walter Gander, "Least squares fit of point clouds," in *Solving Problems in Scientific Computing Using Maple and MATLAB*, 3rd ed., Walter Gander and Jirí Hrebícek, Eds. Berlin, Germany: Spinger, 1997, ch. 23, pp. 339-349.

[237] Pythagoras Papadimitriou, "Two-sided Procrustes-type problems," in *Parallel solution of*

SVD-related problems, with applications. Manchester, UK: PhD thesis, University of Manchester, 1993, ch. 3.

[238] Viveck R. Cadambe and Syed Ali Jafar, "Interference alignment and the degrees of freedom for the K User interference channel," *IEEE Transactions on Information Theory*, pp. 3425-3441, August 2008.

[239] Viveck R. Cadambe and Syed Ali Jafar, "Reflections on interference alignment and the degrees of freedom for the K User interference channel," *IEEE Information Theory Society Newsletter*, vol. 59, no. 4, pp. 5-9, December 2009.

[240] Jinho Choi, "Interference alignment over lattices for MIMO interference channels," *IEEE Communications Letters*, vol. 15, no. 40, pp. 374-376, April 2011.

[241] Bobak Nazer and Michael Gastpar, "Compute-and-forward: a novel strategy for cooperative networks," in *Proc. of the 42nd Annual IEEE Asilomar Conf. on Signals, Systems and Computers*, Monterey, CA, USA, October 2008.

[242] Susanna S. Epp, "Analysis of algorithm efficiency," in *Discrete Mathematics with Applications*, 4th ed. Boston, Massachusetts, USA: Brookes/Cole-Cengage, 2011, ch. 11.

[243] Kaare B. Petersen and Michael S. Pedersen. (2008, February) The Matrix Cookbook. [Online]. http://matrixcookbook.com

[244] Xiaoli Ma and Wei Zhang, "Performance analysis for MIMO systems with lattice-reduction aided linear equalization," *IEEE Transactions on Communications*, vol. 56, no. 2, pp. 309-318, February 2008.

[245] Emmanuel J. Candès and Michael B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21-30, March 2008.

[246] John G. Proakis and Massoud Salehi, *Digital Communications*, 5th ed. New York, New York: McGraw-Hill, 2007, ch. 15.

[247] Marvin K. Simon and Mohamed-Slim Alouini, *Digital Communication over Fading Channels*, 2nd ed. Hoboken, New Jersey, USA: Wiley, 2005.

[248] James A. Anderson, "Lattices," in *Discrete Mathematics with Combinatorics*. Upper Saddle River, New Jersey, USA: Pearson Prentice Hall, 2nd ed., 2004, ch. 9.2-9.3, pp. 357-371.

[249] Gianluigi Ferrari, Guilio Colavolpe, and Riccardo Raheli, *Detection Algorithms for Wireless Communications: With Applications to Wired and Storage Systems*, 43rd ed. Chischester, UK: John Wiley and Sons, 2004, ch. 4.3.

[250] H. Vincent Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. USA: Springer, 1994.

[251] Brian Mazzeo and Michael Rice, "On Monte Carlo simulation of the bit error rate," in *Proc. of ICC'11 - The IEEE Inter. Conf. on Communications*, Kyoto, Japan, 2011.