Algebraic Number Theory and Code Design for Rayleigh Fading Channels

Algebraic Number Theory and Code Design for Rayleigh Fading Channels

Frédérique Oggier

Institut de Mathématiques Bernoulli
École Polytechnique Fédérale de Lausanne
Lausanne 1015, Switzerland
frederique.oggier@epfl.ch

Emanuele Viterbo

Dipartimento di Elettronica Politecnico di Torino
C.so Duca degli Abruzzi 24
Torino 10129, Italy
viterbo@polito.it

the essence of knowledge

Boston – Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1 781 871 0245
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

A Cataloging-in-Publication record is available from the Library of Congress

Printed on acid-free paper

ISBN: 1-933019-07-7; ISSNs: Paper version 1567-2190; Electronic version 1567-2328

Contents

1 Introduction **1**

2 The Communication Problem **5**

2.1 The Fading Channel Model 5
2.2 The Transmission System 6
2.3 Signal Space Diversity and Product Distance 8
2.4 Rotated $\mathbb{Z}^n$–lattice Constellations 11

3 Some Lattice Theory **15**

3.1 First Definitions 15
3.2 Sublattices and Equivalent Lattices 19
3.3 Two Famous Lattices 21
3.4 Lattice Packings and Coverings 23

4 The Sphere Decoder **27**

4.1 The Sphere Decoder Algorithm 28

4.2 The Sphere Decoder with Fading 34
4.3 Conclusions 35

5 First Concepts in Algebraic Number Theory 39

5.1 Algebraic Number Fields 40
5.2 Integral Basis and Canonical Embedding 44
5.3 Algebraic Lattices 48
5.4 Algebraic Lattices over Totally Real Number Fields 53
5.5 Appendix: First Commands in KASH/KANT 54

6 Ideal Lattices 59

6.1 Definition and Minimum Product Distance of an Ideal Lattice 59
6.2 $\mathbb{Z}^n$ Ideal Lattices 62

7 Rotated $\mathbb{Z}^n$–lattices Codes 65

7.1 A Fully Worked Out Example 65
7.2 The Cyclotomic Construction 66
7.3 Mixed Constructions 71
7.4 A Bound on Performance 74
7.5 Some Simulation Results 75
7.6 Appendix: Programming the Lattice Codes 76

8 Other Applications and Conclusions 81

8.1 Dense Lattices for the Gaussian Channel 81
8.2 Complex Lattices for the Rayleigh Fading Channel 82
8.3 Space–Time Block Codes for the Coherent MIMO Channels 82
8.4 Conclusions 84

References 85

1

Introduction

Elementary number theory was the basis of the development of error correcting codes in the early years of coding theory. Finite fields were the key tool in the design of powerful binary codes and gradually entered in the general mathematical background of communications engineers. Thanks to the technological developments and increased processing power available in digital receivers, attention moved to the design of signal space codes in the framework of coded modulation systems. Here, the theory of Euclidean lattices became of great interest for the design of dense signal constellations well suited for transmission over the Additive White Gaussian Noise (AWGN) channel.

More recently, the incredible boom of wireless communications forced coding theorists to deal with fading channels. New code design criteria had to be considered in order to improve the poor performance of wireless transmission systems. The need for bandwidth-efficient coded modulation became even more important due to scarce availability of radio bands. Algebraic number theory was shown to be a very useful mathematical tool that enables the design of good coding schemes for fading channels.

These codes are constructed as multidimensional lattice signal sets (or constellations) with particular geometric properties. Most of the coding gain is obtained by introducing the so-called *modulation diversity* (or *signal space diversity*) in the signal set, which results in a particular type of bandwidth-efficient diversity technique.

Two approaches were proposed to construct high modulation diversity constellations. The first was based on the design of intrinsic high diversity algebraic lattices, obtained by applying the *canonical embedding* of an *algebraic number field* to its *ring of integers*. Only later it was realized that high modulation diversity could also be achieved by applying a particular rotation to a multidimensional QAM signal constellation in such a way that any two points achieve the maximum number of distinct components. Still, these rotations giving diversity can be designed using algebraic number theory.

An attractive feature of this diversity technique is that a significant improvement in error performance is obtained without requiring the use of any conventional channel coding. This can always be added later if required.

Finally, dealing with lattice constellations has also the key advantage that an efficient decoding algorithm is available, known as the *Sphere Decoder*.

Research on coded modulation schemes obtained from lattice constellations with high diversity began more than ten years ago, and extensive work has been done to improve the performance of these lattice codes. The goal of this work is to give both a unified point of view on the constructions obtained so far, and a tutorial on algebraic number theory methods useful for the design of algebraic lattice codes for the Rayleigh fading channel.

This paper is organized as follows. Chapter 2 is dedicated to the communication problem. All the assumptions on the system model and the code design criteria are detailed there. We motivate the choice of lattice codes for this model.

Since some basic knowledge of lattices is required for the code constructions, Chapter 3 recalls elementary definitions and properties of lattices.

A very important feature to consider when designing codes is their decoding. Application of arbitrary lattice codes became attractive thanks to the *Sphere Decoder*, a universal lattice decoding algorithm, described in Chapter 4 in its original form.

Chapter 5 is a self-contained short introduction to algebraic number theory. It starts from the very elementary definitions, and focuses on the construction of *algebraic lattices*.

Chapter 6 introduces the key notion of *ideal lattice*, which gives a unifying context for understanding algebraic lattice codes. It allows the construction of close form expressions for the key performance parameters of lattice codes in terms of algebraic properties of the underlying number field.

At this point, we have all the mathematical tools to build efficient lattice codes. Some explicit constructions are given and their performance is shown in Chapter 7. Once again, the algebraic properties of the lattice will help us in deriving a bound on the performance, which we will use to show that known lattices codes are almost optimal, and that no significant further improvement can be achieved.

In Chapter 8, we give a brief overview of other applications of the theory of algebraic lattice codes; for instance, complex lattice codes can be used similarly to the real ones in the case where we assume complex fading coefficients. Finally, we give an example of algebraic space–time block code, to illustrate how this theory can be generalized and used in the context of cyclic division algebras for designing codes for MIMO channels. This last application is a promising area of research, and we give here an example to motivate further investigations.

For readers interested in implementing the constructions of algebraic lattice codes, we add at the end of Chapters 5 and 7 some commands in KASH/KANT, a computational algebra software tool. In such a programming language, all the elementary algorithms for number field computations are readily available.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Transactions on Information Theory*, vol. 48, n. 8, pp. 2201–2214, 2002.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, “PARI/GP – a software package for computer-aided number theory,”. Available at http://www.math.u-psud.fr/~belabas/pari/.

[3] E. Bayer-Fluckiger, “Lattices and number fields,” *Contemporary Mathematics*, vol. 241, pp. 69–84, 1999.

[4] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, “New algebraic constructions of rotated $\mathbb{Z}^n$–lattice constellations for the Rayleigh fading channel,” *IEEE Transactions on Information Theory*, vol. 50, n. 4, pp. 702–714, 2004.

[5] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, “Algebraic lattice constellations: Bounds on performance,” *submitted to IEEE Transactions on Information Theory*, April 2004.

[6] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, “Bounds on the performance of rotated lattice constellations,” *Proceedings of the IEEE International Symposium on Information Theory*, April 2004.

[7] J.-C. Belfiore and G. Rekaya, “Quaternionic lattices for space-time coding,” *Proceedings of ITW2003, Paris*, April 2003.

[8] J.-C. Belfiore, G. Rekaya, and E. Viterbo, “The Golden code: A 2x2 full-rate space-time code with non-vanishing determinants,” *Proceedings of the IEEE International Symposium on Information Theory*, 2004.

[9] K. Boullé and J.-C. Belfiore, “Modulation schemes designed for the Rayleigh channel,” *Proc. CISS, Princeton, NJ*, pp. 288–293, 1992.

[10] J. Boutros, “Constellations optimales par plongement canonique,” *Mémoire de fin d’études, E.N.S.T. Paris*, 1992.
[11] J. Boutros, “Réseaux de points pour les canaux à évanouissements,” *Ph.D. thesis, E.N.S.T. Paris*, 1996.
[12] J. Boutros and E. Viterbo, “High diversity lattices for fading channels,” *Proceedings 1995 IEEE International Symposium on Information Theory*, 1995.
[13] J. Boutros and E. Viterbo, “New approach for transmission over fading channel,” *Proceedings of ICUPC’96*, pp. 66–70, 1996.
[14] J. Boutros and E. Viterbo, “Number fields and modulations for the fading channel,” *presented at the workshop Réseaux Euclidiens et Formes Modulaires, Colloque CIRM, Luminy*, 1996.
[15] J. Boutros and E. Viterbo, “Rotated multidimensional QAM constellations for Rayleigh fading channels,” *Proceedings of the 1996 IEEE Information Theory Workshop*, 1996.
[16] J. Boutros and E. Viterbo, “Rotated trellis coded lattices,” *Proceedings of the XXVth General Assembly of the International Union of Radio Science, URSI*, 1996.
[17] J. Boutros and E. Viterbo, “Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel,” *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1453–1467, 1998.
[18] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, “Good lattice constellations for both Rayleigh fading and gaussian channels,” *IEEE Transactions on Information Theory*, vol. 42, n. 2, pp. 502–518, 1996.
[19] J. Boutros and M. Yubero, “Converting the Rayleigh fading channel into a Gaussian channel,” *Mediterranean Workshop on Coding and Information Integrity*, 1996.
[20] L. Brunel and J. Boutros, “Lattice decoding for joint detection in direct-sequence cdma systems,” *IEEE Transactions on Information Theory*, pp. 1030–1037, 2003.
[21] H. Cohen, *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.
[22] H. Cohn, *Advanced Number Theory.* Dover Publications, New York, 1980.
[23] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* Springer-Verlag, New York, 1988.
[24] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, “Kant v4,” *J. Symbolic Comp.*, vol. 24, pp. 267–283, 1997.
[25] M. O. Damen, A. Chkeif, and J.-C. Belfiore, “Lattice code decoder for space-time codes,” *IEEE Communications Letters*, vol. 4, n. 5, pp. 161–163, 2000.
[26] M. O. Damen, H. El Gamal, and G. Caire, “On maximum-likelihood detection and the search for the closest lattice point,” *IEEE Transactions on Information Theory*, vol. 49, n. 10, pp. 2389–2402, 2003.
[27] 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, pp. 463–471, 1985.

[28] G. D. Forney Jr., "Multidimensional constellations. ii. Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, n. 6, pp. 941–958, 1989.

[29] X. Giraud, "Constellations pour le canal à évanouissements," *Ph.D. thesis, E.N.S.T. Paris*, 1994.

[30] X. Giraud and J.-C. Belfiore, "Constellation design for Rayleigh fading channels," *Proceedings of the 1996 IEEE Information Theory Workshop*, p. 25, 1996.

[31] X. Giraud and J.-C. Belfiore, "Constellations matched to the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 42, n. 1, pp. 106–115, 1996.

[32] X. Giraud, K. Boullé, and J.-C. Belfiore, "Constellations designed for the Rayleigh fading channel," *Proceedings of ISIT'93*, p. 342, 1993.

[33] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Transactions on Information Theory*, vol. 43, n. 3, pp. 938–952, 1997.

[34] Giraud, X. and Belfiore, J.-C., "Coset codes on constellations matched to the fading channel," *Proceedings of ISIT'94*, p. 26, 1994.

[35] B. Hassibi and H. Vikalo, "On the expected complexity of sphere decoding," *Thirty-Fifth Asilomar Conference on Signals, Systems and Computers*, vol. 2, n. 4-7, pp. 1051–1055, 2001.

[36] B. Jeličić and S. Roy, "Design of a trellis coded QAM for flat fading and AWGN channels," *IEEE Transactions on Vehicular Technology*, vol. 44, n. 1, 1995.

[37] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1994.

[38] Odlyzko, A. M., "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results," *Séminaire de Théorie des Nombres, Bordeaux*, pp. 1–15, 1989.

[39] F. Oggier and E. Bayer-Fluckiger, "Best rotated cubic lattice constellations for the Rayleigh fading channel," *Proceedings of the IEEE International Symposium on Information Theory*, 2003.

[40] M. Pohst, "KASH/KANT-computer algebra system,". Technische Universität, Berlin, Available at http://www.math.tu-berlin.de/algebra/.

[41] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications," *ACM SIGSAM Bulletin*, vol. 15, pp. 37–44, 1981.

[42] M. Pohst, *Computational algebraic number theory.* DMV Seminar, vol. 21, Birkhäuser Verlag, 1993.

[43] P. Samuel, *Théorie Algébrique des Nombres.* Hermann, 1971.

[44] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Transactions on Information Theory*, vol. 49, n. 10, October 2003.

[45] I. N. Stewart and D. O. Tall, *Algebraic Number Theory.* Chapman and Hall, 1979.

[46] H. P. F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory.* University Press of Cambridge, 2001.

[47] G. Taricco and E. Viterbo, "Performance of component interleaved signal sets for fading channels," *Electronics Letters*, vol. 32, n. 13, pp. 1170–1172, October 1996.

[48] G. Taricco and E. Viterbo, "Performance of high diversity multidimensional constellations," *IEEE International Symposium on Information Theory*, October 1997.

[49] G. Taricco and E. Viterbo, "Performance of high diversity multidimensional constellations," *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1539–1543, July 1998.

[50] E. Viterbo, "Tecniche matematiche computazionali per l'analisi ed il progetto di costellazioni a reticolo," *Ph.D. thesis, Politecnico di Torino*, 1995.

[51] E. Viterbo and E. Biglieri, "A universal lattice decoder," 14^{eme} *Colloque GRETSI*, pp. 611–614, 1993.

[52] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Transactions on Information Theory*, vol. 45, n. 5, pp. 1639–1642, 1999.

[53] L. C. Washington, *Introduction to Cyclotomic Fields.* Springer-Verlag, NY, 1982.

[54] M. A. Yubero, "Réseaux de points à haute diversité," *Proyecto fin de carrera, Escuele Técnica Superior de Ingenieros de Telecomunicación, Madrid Spain*, 1995.

Index

$d_{p,min}$, 9
l-product distance, 9

abelian group, 16
algebraic element, 39
algebraic extension, 40
algebraic integer, 41
algebraic number field, 40

basis of a lattice, 16
bit labeling, 11

canonical embedding, 45
Channel State Information, 5
commutative ring, 38
conjugates, 43
constellation shaping, 11
coset, 19
CSI, 5
cyclotomic field, 65

degree, 39
determinant of a lattice, 17
discriminant, 44
diversity order, 9

embedding, 43
equivalent lattice, 21

field, 38
field extension, 39
finite extension, 39
fundamental parallelotope, 16

generator matrix, 17
Gram matrix, 17
group, 15

ideal, 49
ideal lattice, 57
in-phase/quadrature component interleaver,

6
index of a lattice, 19
integral basis, 42
integral lattice, 17
invariant of a lattice, 17

lattice, 16

maximal diversity, 9
maximal real subfield of a cyclotomic field, 65
Maximum Likelihood, 8
minimal polynomial, 39
ML, 8
modulation diversity, 9

norm, 44
norm of an ideal, 50
number field, 39

principal ideal, 49

quotient group, 19

ring, 38
ring homomorphism, 43
ring of integers, 41

scaled lattice, 20
signature, 45
skew field, 38
subgroup, 16
sublattice, 19

totally complex, 45
totally real, 45
trace, 44

units of a ring, 38

volume of a lattice, 18