Cyclic Division Algebras: A Tool for Space–Time Coding

Cyclic Division Algebras: A Tool for Space–Time Coding

Frédérique Oggier

California Institute of Technology
Pasadena CA-91125
frederique@systems.caltech.edu

Jean-Claude Belfiore

École Nationale Supérieure des Télécommunications
75013 Paris
France
belfiore@enst.fr

Emanuele Viterbo

Università della Calabria
Italy
viterbo@deis.unical.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. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

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

The preferred citation for this publication is F. Oggier, J.-C. Belfiore and E. Viterbo, Cyclic Division Algebras: A Tool for Space–Time Coding, Foundations and Trends® in Communications and Information Theory, vol 4, no 1, pp 1–95, 2007

ISBN: 978-1-60198-050-2

Foundations and Trends® in Communications and Information Theory
Volume 4 Issue 1, 2007

Editorial Scope

Foundations and Trends® in Communications and Information Theory will publish survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2007, Volume 4, 6 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328. Also available as a combined paper and online subscription.

Foundations and Trends® in
Communications and Information Theory
Vol. 4, No. 1 (2007) 1–95

DOI: 10.1561/0100000016

Cyclic Division Algebras: A Tool for Space–Time Coding

Frédérique Oggier[1], Jean-Claude Belfiore[2], and Emanuele Viterbo[3]

[1] *Department of Electrical Engineering, California Institute of Technology, Pasadena CA-91125, frederique@systems.caltech.edu*
[2] *École Nationale Supérieure des Télécommunications, 46 rue Barrault, 75013 Paris, France, belfiore@enst.fr*
[3] *Dipartimento di Elettronica, Informatica e Sistemistica, Università della Calabria, Arcavacata di Rende, Italy, viterbo@deis.unical.it*

Abstract

Multiple antennas at both the transmitter and receiver ends of a wireless digital transmission channel may increase both data rate and reliability. Reliable high rate transmission over such channels can only be achieved through Space–Time coding. Rank and determinant code design criteria have been proposed to enhance diversity and coding gain. The special case of *full-diversity* criterion requires that the difference of any two distinct codewords has full rank.

Extensive work has been done on Space–Time coding, aiming at finding fully diverse codes with high rate. Division algebras have been proposed as a new tool for constructing Space–Time codes, since they are non-commutative algebras that naturally yield linear fully diverse codes. Their algebraic properties can thus be further exploited to improve the design of good codes.

The aim of this work is to provide a tutorial introduction to the algebraic tools involved in the design of codes based on cyclic division algebras. The different design criteria involved will be illustrated, including the constellation shaping, the information lossless property, the non-vanishing determinant property, and the diversity multiplexing trade-off. The final target is to give the complete mathematical background underlying the construction of the Golden code and the other Perfect Space–Time block codes.

Keywords: Cyclic algebras; division algebras; full diversity; golden code; non-vanishing determinant; perfect space–time codes; space–time coding.

Contents

1

Introduction

Algebraic coding has played an important role since the early age of coding theory. Error correcting codes for the binary symmetric channel were designed using finite fields and codes for the additive white Gaussian channel were designed using Euclidean lattices.

The introduction of wireless communication required new coding techniques to combat the effect of fading channels. Modulation schemes based on algebraic number theory and the theory of algebraic lattices were proposed for single antenna Rayleigh fading channels thanks to their intrinsic modulation diversity.

New advances in wireless communications led to consider systems with multiple antennas at both the transmitter and receiver ends, in order to increase the data rates. The coding problem became more complex and the code design criteria for such scenarios showed that the challenge was to construct *fully-diverse* codes, i.e., sets of matrices such that the difference of any two distinct matrices is full rank. This required new tools, and from the algebraic side, *division algebras* quickly became prominent.

1.1 Division Algebra Based Codes

Division algebras are non-commutative algebras that naturally yield families of fully-diverse codes, thus enabling to design high rate, highly reliable Space–Time codes, which are characterized by many optimal features, deeply relying on the algebraic structures of the underlying algebra.

The idea of using division algebras was first introduced in [51], where so-called Brauer algebras were presented, and in [50], where it was shown that the acclaimed Alamouti code [1] can actually be built from a simple example of division algebras, namely the Hamilton quaternions. Quaternion algebras were more generally used in [6], where the notion of non-vanishing determinant was introduced.

Different code constructions appeared then in [52], based on field extensions and cyclic algebras. In [7, 44] and then in [21], perfect codes were presented as division algebra codes which furthermore satisfy a shaping property and have a non-vanishing determinant. In [53], information lossless codes from crossed product algebras, a new family of division algebras, are presented. In [31], codes from maximal orders of division algebras are investigated. In [39] some non-cubic shaping, non-vanishing determinant codes are proposed based on cyclic division algebras.

In parallel, in [7, 15, 33, 63], the first 2×2 codes achieving the diversity-multiplexing gain trade-off of Zheng and Tse [64] were found. It was furthermore shown [63] that a necessary condition to achieve the trade-off for a 2×2 code is actually to have a non-vanishing determinant (though not stated with this terminology). In [7], it was shown that the algebraic structure of cyclic division algebras was the key for constructing 2×2 non-vanishing determinant codes. In [20], it was shown more generally that division algebra codes are a class of codes that achieve the trade-off, thanks to the non-vanishing determinant.

All the notions mentioned in the above short history of division algebra based codes will be explained in this work. We will focus on cyclic division algebras, a particular family of division algebras. These will be built over number fields, with base field $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$, with $i^2 = -1$ and $j^3 = 1$, which are suitable to describe QAM or HEX constellations.

The notion of constellation *shaping* will be explained, thanks to an underlying lattice structure. We will show how this is related to the information lossless property. Furthermore, having $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$ as a base field will allow us to get the so-called *non-vanishing determinant* property, which will be shown to be a sufficient condition to reach the *diversity-multiplexing trade-off*.

1.2 Organization

This paper is organized as follows. Chapter 2 details the channel model considered. It recalls the two main code design criteria derived from the pairwise probability of error, namely: the *rank criterion* and the *determinant criterion*. It then discusses the modulations used, QAM and HEX constellations. Decoding is furthermore considered, which also enlightens the importance of the *constellation shaping* in the code performance.

In Chapter 3, performance of the code is considered from an information theoretic perspective. The goal is to explain the role of the *diversity-multiplexing gain* trade-off, as well as the *information lossless* property, which guarantees that a coded system will have the same capacity as an uncoded one assuming QAM input symbols.

Chapters 2 and 3 give a characterization of the properties a Space–Time code should achieve to be efficient. Codes based on cyclic division algebras have been shown to fulfill those properties. Their construction is however involved, and it is the goal of Chapter 4 to introduce the algebra background necessary to construct those codes. No algebra background is required to read this chapter. Division algebras are introduced, as well as *number fields*. We also define concepts such as *algebraic norm* and *algebraic trace*, that will be important for the code construction.

Once the algebra background is set, Chapter 5 explains the construction of the Golden code and some other Perfect Space–Time block codes for small number of antennas, namely up to six.

The last chapter briefly presents future applications of those techniques, toward coding for wireless networks, and trellis/block coded modulations.

References

[1] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas Communications*, vol. 16, pp. 1451–1458, October 1998.

[2] K. Azarian, H. El Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Transactions on Information Theory*, vol. 51, no. 12, December 2005.

[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, no. 4, pp. 702–714, 2004.

[5] J.-C. Belfiore and A. M. Cipriano, "Space-time coding for non-coherent channels," in *Space-Time Wireless Systems: From Array Processing to MIMO Communications*, (H. Boelcskei, D. Gesbert, C. Papadias, and A. J. van der Veen, eds.), ch. 10, Cambridge University Press, June 2006.

[6] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proceedings of ITW 2003*, Paris, April 2003.

[7] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2×2 full-rate space-time code with non-vanishing determinants," *IEEE Transactions on Information Theory*, vol. 51, no. 4, April 2005.

[8] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: Information-theoretic and communications aspects," *IEEE Transactions on Information Theory*, vol. 44, no. 6, 1998.

[9] H. Bolcskei and A. Paulraj, "Space-frequency codes for broadband fading channels," in *Proceedings of ISIT 2001*, p. 219, Washington DC, June 2001.

[10] D. Champion, J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Partitionning the golden code: A framework to the design of space-time coded modulation," *Canadian Workshop on Information Theory*, Montreal, 2006.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag, 1988.

[12] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 628–636, March 2002.

[13] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *Communications Letters*, vol. 4, pp. 161–163, May 2000.

[14] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Transactions on Information Theory*, vol. 48, pp. 753–760, March 2002.

[15] P. Dayal and M. K. Varanasi, "An optimal two transmit antenna space-time code and its stacked extensions," in *Proceedings of Asilomar Conference on Signals, Systems and Computers*, 2003.

[16] P. Dayal and M. K. Varanasi, "Distributed QAM-based space-time block codes for efficient cooperative multiple-access communication," *submitted to IEEE Transactions on Information Theory, accepted for publication*, March 2006.

[17] H. El Gamal, G. Caire, and M. O. 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, 2004.

[18] H. El Gamal and M. Damen, "Universal space-time coding," *IEEE Transactions on Information Theory*, vol. 49, no. 5, May 2003.

[19] P. Elia, P. V. Oggier, and F. Kumar, "Asymptotically optimal cooperative wireless networks with reduced signaling complexity," *Special Issue on the IEEE Journal on Selected Areas in Communications on Cooperative Communications and Networking*, vol. 25, no. 2, February 2007.

[20] P. Elia, K. Raj Kumar, S. A. Pawar, P. Vijay Kumar, and H.-F. Lu, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Transactions on Information Theory*, vol. 52, no. 9, September 2006.

[21] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space-time codes with minimum and non-minimum delay for any number of antennas," *International Conference on Wireless Networks, Communications and Mobile Computing*, 2005.

[22] G. D. Forney, R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient modulation for band-limited channels," *IEEE Journal on Selected Areas in Communications*, vol. 2, pp. 632–647, September 1984.

[23] G. D. Forney and L.-F. Wei, "Multidimensional constellations. I. Introduction, figures of merit, and generalized cross constellations," *IEEE Journal on Selected Areas Communications*, vol. 7, pp. 877–892, August 1989.

[24] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Techical Journal*, pp. 41–59, 1996.

[25] G. J. Foschini and M. J. Gans, "On limits of wireless communication in a fading environment when using multiple antennas," *Wireless Personal Communications*, pp. 311–335, March 1998.

[26] A. R. Hammons and H. El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 524–542, October 2000.

[27] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Transactions on Information Theory*, vol. 48, pp. 1804–1824, July 2002.

[28] B. Hassibi and H. Vikalo, "On sphere decoding algorithm. I. Expected complexity," *IEEE Transactions on Signal Processing*, vol. 53, pp. 2806–2818, August 2005.

[29] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Transactions on Information Theory*, vol. 46, pp. 543–564, March 2000.

[30] C. Hollanti and J. Lahtonen, "Maximal orders in the design of dense space-time lattice codes," *submitted to IEEE Transactions on Information Theory*, September 2006.

[31] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras," in *Proceedings of ISIT*, Seattle, 2006.

[32] Y. Hong, E. Viterbo, and J.-C. Belfiore, "Golden space-time trellis coded modulation," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1689–1705, May 2007.

[33] A. Hottinen, O. Tirkkonen, and R. Wichman, *Multi-Antenna Transceiver Techniques for 3G and Beyond*. John Wiley & Sons Ltd, 2003.

[34] Y. Jing and B. Hassibi, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless network," *IEEE Transactions on Information Theory*, vol. 49, October 2003.

[35] Y. Jing and B. Hassibi, "Distributed space-time coding in wireless relay networks," *IEEE Transactions on Wireless Communications*, vol. 5, December 2006.

[36] T. Kiran and B. Sundar Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Transactions on Information Theory*, vol. 51, no. 8, August 2005.

[37] T. Kiran and B. Sundar Rajan, "Distributed space-time codes with reduced decoding complexity," in *Proceedings of ISIT*, Seattle, 2006.

[38] X.-B. Liang, "Orthogonal designs with maximal rates," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2468–2503, October 2003.

[39] H. Liao and X.-G. Xia, "Some designs of full rate Space-Time codes with non-vanishing determinant," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2898–2908, 2007.

[40] H.-F. Lu and P. Vijay Kumar, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1709–1730, 2005.

[41] F. Oggier, "On the optimality of the golden code," in *Proceedings of the Information Theory Workshop*, Chengdu, 2006.

[42] F. Oggier and B. Hassibi, "An algebraic coding scheme for wireless relay networks with multiple-antenna nodes," *submitted to IEEE Transactions on Signal Processing*, March 2006.

[43] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Foundations and Trends in Communications and Information Theory*, vol. 1, 2004.

[44] F. E. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Transactions on Information Theory*, vol. 52, no. 9, September 2006.

[45] R. S. Pierce, *Associative Algebras.* New York: Springer-Verlag, 1982.

[46] K. Raj Kumar and G. Caire, "Construction of structured LaST codes," in *Proceedings of ISIT*, pp. 2834–2838, Seattle, 2006.

[47] K. Raj Kumar, S. A. Pawar, P. Elia, P. Vijay Kumar, and B. Sethuraman, "Codes achieving the DM tradeoff of the MIMO-ARQ Channel," in *Proceedings of IEEE International Symposium on Information Theory*, pp. 901–905, Adelaide, September 2005.

[48] P. Samuel, *Théorie algébrique des nombres.* Hermann, 1971.

[49] W. Scharlau, *Quadratic and Hermitian Forms.* Springer Verlag, 1985.

[50] B. A. Sethuraman and B. Sundar Rajan, "An algebraic description of orthogonal designs and the uniqueness of the alamouti code," in *Proceedings of the Global Telecommunications Conference*, 2002.

[51] B. A. Sethuraman and B. Sundar Rajan, "Full-rank, full-rate STBCs from division algebras," in *Proceedings of the Information Theory Workshop*, Bangalore, 2002.

[52] 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, no. 10, October 2003.

[53] V. Shashidhar, B. Sundar Rajan, and B. A. Sethuraman, "Information-lossless space-time block codes From crossed-product algebras," *IEEE Transactions on Information Theory*, vol. 52, no. 9, September 2006.

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

[55] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal design," *IEEE Transactions on Information Theory*, vol. 45, pp. 1456–1466, July 1999.

[56] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, pp. 744–765, March 1998.

[57] S. Tavildar and P. Viswanath, "Approximately universal codes over slow fading channels," *IEEE Transactions on Information Theory*, vol. 57, July 2006.

[58] E. Telatar, "Capacity of multi-antenna gaussian channels," *European Transactions on Telecommunications ETT*, pp. 585–596, November 1999.

[59] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* Cambridge University Press, 2006.

[60] E. Viterbo and J. Boutros, “A universal lattice code decoder for fading channels,” *IEEE Transactions on Information Theory*, vol. 45, pp. 1639–1642, July 1999.

[61] 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 *International Symposium on Signal, Systems and Electronics*, pp. 295–300, September 1998.

[62] S. Yang and J.-C. Belfiore, “Optimal space-time codes for the amplify-and-forward cooperative channel,” *IEEE Transactions on Information Theory*, vol. 53, February 2007.

[63] H. Yao and G. W. Wornell, “Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes,” in *Proceedings of Allerton Conference on Communication, Control and Computing*, 2003.

[64] L. Zheng and D. N. C. Tse, “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels,” *IEEE Transactions on Information Theory*, vol. 49, pp. 1073–1096, May 2003.