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

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

© 2007 F. Oggier, J.-C. Belfiore and E. Viterbo

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1-781-871-0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Full text available at: http://dx.doi.org/10.1561/0100000016
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.
Cyclic Division Algebras: A Tool for Space–Time Coding

Frédérique Oggier¹, Jean-Claude Belfiore², and Emanuele Viterbo³

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.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2 Algebras on Number Fields</td>
<td>45</td>
</tr>
<tr>
<td>4.3 Norm and Ring of Integers</td>
<td>55</td>
</tr>
<tr>
<td>4.4 Shaping, Lattices and Discriminant</td>
<td>61</td>
</tr>
<tr>
<td>5 Perfect Space–Time Block Codes</td>
<td>69</td>
</tr>
<tr>
<td>5.1 Definition of Perfect Space–Time Codes</td>
<td>69</td>
</tr>
<tr>
<td>5.2 The Golden Code</td>
<td>72</td>
</tr>
<tr>
<td>5.3 A Perfect STBC for 3 Antennas</td>
<td>75</td>
</tr>
<tr>
<td>5.4 A Perfect STBC for 4 Antennas</td>
<td>77</td>
</tr>
<tr>
<td>5.5 A Perfect STBC for 5 Antennas</td>
<td>79</td>
</tr>
<tr>
<td>5.6 A Perfect STBC for 6 Antennas</td>
<td>81</td>
</tr>
<tr>
<td>5.7 Optimality of Perfect STBCs</td>
<td>83</td>
</tr>
<tr>
<td>6 New Applications and Conclusion</td>
<td>85</td>
</tr>
<tr>
<td>6.1 Coding for Wireless Networks</td>
<td>85</td>
</tr>
<tr>
<td>6.2 Trellis/Block Coded Modulations</td>
<td>87</td>
</tr>
<tr>
<td>6.3 Other Issues</td>
<td>88</td>
</tr>
<tr>
<td>6.4 Conclusion</td>
<td>89</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>91</td>
</tr>
<tr>
<td>References</td>
<td>93</td>
</tr>
</tbody>
</table>
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 $2 \times 2$ 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 $2 \times 2$ 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 $2 \times 2$ 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.
1.2 Organization

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


References


References


