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

DOI: 10.1561/0100000016

now
the essence of knowledge

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.

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.

2

The MIMO System Model

2.1 Introduction

Multiple transmit and multiple receive antennas have emerged as a promising technique for improving the performance of wireless digital transmission systems [25, 58]. The limited resources of a wireless communication system, such as spectrum and power, can be efficiently used with multiple antennas to provide good quality and large capacity to a wide range of applications requiring high data rate.

Multiple antenna systems are described by a multiple-input multiple output (MIMO) system model, where the propagation environment is a quasi-static and frequency-flat Rayleigh fading channel [8]. This assumption is necessary to establish simple code design criteria. Nevertheless, the codes designed under this simplifying assumption yield good performance in a wide variety of real world scenarios.

Consider a system with n_t transmit antennas and n_r receive antennas. The complex baseband channel, within a single fading block of T symbol durations, can be expressed as

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \mathbf{X}_{n_t \times T} + \mathbf{Z}_{n_r \times T}. \tag{2.1}$$

The subscripts indicate the corresponding matrix dimensions and will be omitted for simplicity in the following. The h_{ij} element of the channel matrix $\mathbf{H}$ corresponds to the channel coefficient between the jth transmit and the ith receive antenna and it is modeled as a complex Gaussian random variable with zero mean and unit variance $\mathcal{N}_c(0,1)$.

The matrix $\mathbf{Z}$ corresponds to the spatially and temporally additive white noise, whose independent entries are complex Gaussian random variables $\mathcal{N}_c(0,N_0)$, where N_0 is the noise power spectral density. The x_{ik} entry of $\mathbf{X}$ corresponds to the signal transmitted from the ith antenna during the kth symbol interval for $1 \leq k \leq T$. We let the time T coincide with the *coherence time*, i.e., the time during which the channel coefficients remain constant. It is also assumed that $\mathbf{H}$ is independent of both $\mathbf{X}$ and $\mathbf{Z}$.

Let $E_s = \mathbb{E}[|x_{ik}|^2]$ denote the signal energy transmitted from each antenna. We define the *signal-to-noise ratio* (SNR) at the receiver as

$$\frac{\mathbb{E}\left[\|\mathbf{HX}\|^2\right]}{\mathbb{E}\left[\|\mathbf{Z}\|^2\right]} = \frac{n_t E_s}{N_0}, \tag{2.2}$$

where $\|\cdot\|$ denotes the Frobenius norm of the matrix argument. For this kind of channels, the capacity at high SNR scales with $\min(n_t, n_r)$, [25]:

$$C(n_t, n_r, \mathsf{SNR}) \sim \min(n_t, n_r)\log(\mathsf{SNR}). \tag{2.3}$$

This means that by using appropriate processing, the additional spatial degrees of freedom (with respect to single transmit single receive antenna) allow the transmission of independent data flows through the channel and the separation of these flows at the receiver side. Equation (2.3) indicates how MIMO techniques enable the data rate of wireless systems to increase. In fact, we can observe that MIMO offers approximately $\min(n_t, n_r)$ parallel spatial channels between the transmitter and the receiver. Several schemes have been proposed to effectively exploit this spatial multiplexing [24, 61].

In the case of sufficiently spaced transmit and receive antenna arrays, the $n_t n_r$ channels between all pairs of transmit and receive antennas are independent. This suggests that MIMO can be also used to combat fading using *diversity* techniques, i.e., different independently

faded replicas of the information symbols are sent over the independent channels and are available at the receiver side. In other words, a signal is lost only when all its copies are lost, resulting in higher immunity against channel fades.

A maximum diversity advantage of $n_t n_r$, corresponding to the number of channels between the transmitter and the receiver, can be achieved. In order to exploit the transmit diversity, several *Space–Time Block Codes* (STBC) have been proposed in the literature [1, 12, 14, 26, 27, 33, 38, 40, 55]. *Space–Time Trellis Codes* (STTC) have also been extensively studied in the literature developing from [56]. In this work, we will focus on algebraic constructions of STBCs.

Note that the terminology *Space–Time Codes* for multiple antennas codes comes from the fact that we are indeed coding over "space" (since we have several antennas) and "time." The same codes can be applied over a multipath channel by swapping time with frequency and using a multicarrier modulation technique such as OFDM. In this setting these codes are known as *Space-Frequency codes* [9].

2.2 Design Criteria for Space–Time Codes

Design criteria for Space–Time codes depend on the type of receiver that is considered. Two major classes of receivers have been considered in the literature: *coherent* and *non-coherent*. In the first case, considered throughout this work, it is assumed that the receiver has recovered the exact information about the state of the channel (this is also known as perfect Channel State Information (CSI)). In practice this can be obtained by introducing some pilot symbols that enable accurate channel estimation, so that we can assume that the channel matrix $\mathbf{H}$ is known at the receiver. For the non-coherent case, many different solutions are available and we address the reader to [5, 29].

Definition 2.1. An STBC is a finite set $\mathcal{C}$ of $n_t \times T$ complex matrices $\mathbf{X}$ and we denote by $|\mathcal{C}|$ the cardinality of the *codebook*.

Under the assumption of perfect CSI, *maximum likelihood* (ML) decoding corresponds to choosing the codeword $\mathbf{X}$ that minimizes the

squared Frobenius norm:

$$\min_{\mathbf{X}\in\mathcal{C}} \|\mathbf{Y} - \mathbf{H}\mathbf{X}\|^2 .$$

An estimate of the error probability $P(e)$ can be obtained using the *union bound*

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{\mathbf{X}\in\mathcal{C}} \sum_{\hat{\mathbf{X}}\neq\mathbf{X}} P(\mathbf{X} \to \hat{\mathbf{X}}), \tag{2.4}$$

where $P(\mathbf{X} \to \hat{\mathbf{X}})$ is the *pairwise error probability*, i.e., the probability that, when a codeword $\mathbf{X}$ is transmitted, the ML receiver decides erroneously in favor of another codeword $\hat{\mathbf{X}}$, assuming only $\mathbf{X}$ and $\hat{\mathbf{X}}$ are in the codebook. It can be shown that

$$P(\mathbf{X} \to \hat{\mathbf{X}}) = \mathbb{E}\left[\mathcal{Q}\left(\frac{\|\mathbf{H}(\mathbf{X} - \hat{\mathbf{X}})\|}{\sqrt{2N_0}}\right)\right], \tag{2.5}$$

where $\mathcal{Q}$ is the Gaussian tail function, $\mathbf{X} - \hat{\mathbf{X}}$ is the *codeword difference matrix* and the average is over all realizations of $\mathbf{H}$.

In the case of independent Rayleigh fading ($h_{ij} \sim \mathcal{N}_c(0,1)$), we can write

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq \det\left[\mathbf{I}_{n_t} + \frac{(\mathbf{X} - \hat{\mathbf{X}})(\mathbf{X} - \hat{\mathbf{X}})^\dagger}{4N_0}\right]^{-n_r}. \tag{2.6}$$

Let r denote the rank of the codeword difference matrix. If $r = n_t$ for all pairs $(\mathbf{X}, \hat{\mathbf{X}})$, we say that the code is *full rank*. If we denote by $\lambda_j, j = 1, \ldots, r$ the non-zero eigenvalues of the *codeword distance matrix*

$$\mathbf{A} = (\mathbf{X} - \hat{\mathbf{X}})(\mathbf{X} - \hat{\mathbf{X}})^\dagger \tag{2.7}$$

we can rewrite (2.6) as

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq \prod_{j=1}^{r} \left(1 + \frac{\lambda_j}{4N_0}\right)^{-n_r}. \tag{2.8}$$

For high signal-to-noise ratios (small N_0), we have

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq \Delta^{-n_r} \left(\frac{1}{4N_0}\right)^{-rn_r}, \tag{2.9}$$

where $\Delta = \prod_{j=1}^{r} \lambda_j$. Then we can write

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq \left(\frac{\Delta^{1/r}}{4N_0} \right)^{-rn_r}. \tag{2.10}$$

In the union bound (2.4) the asymptotically dominant terms in the sum have the lowest exponent rn_r.

Definition 2.2. We call $\min\{rn_r\}$ the *diversity gain* of the code, which represents the asymptotic negative slope of the error probability in a log–log scale plot versus SNR.

In the case of full rank codes ($r = n_t$), we have

$$\Delta = \prod_{j=1}^{n_t} \lambda_j = \det(\mathbf{A}) \neq 0 \text{ for all } \mathbf{A}$$

and we say that the code has *full diversity*. This means that we can exploit all the $n_t n_r$ independent channels available in the MIMO system.

It is well known that the truncated union bound, taking into account only some of the terms in the sum (2.4), is not very accurate with fading channels. Nevertheless it provides a reasonably simple code design criterion if only the dominant term in the sum is considered. In the case of full diversity codes, the dominant term in the union bound (2.4) is given by the so called *minimum determinant* of the code,

$$\Delta_{\min} = \min_{\mathbf{X} \neq \hat{\mathbf{X}}} \det(\mathbf{A}). \tag{2.11}$$

The term $(\Delta_{\min})^{1/n_t}$ is also known as the *coding gain* [56].

Definition 2.3. We define a *linear* STBC as an STBC $\mathcal{C}$ such that

$$\forall\ \mathbf{X}, \mathbf{X}' \in \mathcal{C}\ \ \mathbf{X} \pm \mathbf{X}' \in \mathcal{C}.$$

This linearity property can only be true for an *infinite code* $\mathcal{C}_\infty$, i.e., a code with an infinite number of codewords.

This definition parallels the one of lattice constellations carved from infinite lattices: a finite STBC can be carved from a linear STBC. We will see below that the performance analysis of these codes can be greatly simplified.

In the case of linear codes the sum or difference of any pair of codewords is a codeword, hence the union bound reduces to

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{\mathbf{X} \neq \mathbf{0}} P(\mathbf{0} \to \mathbf{X}) \tag{2.12}$$

and we have

$$\Delta_{\min} = \min_{\mathbf{X} \neq \mathbf{0}_{n_t \times T}} \det\left(\mathbf{X}\mathbf{X}^{\dagger}\right). \tag{2.13}$$

A finite STB code $\mathcal{C} \subset \mathcal{C}_{\infty}$ has a minimum determinant $\Delta_{\min}(\mathcal{C}) \geq \Delta_{\min}(\mathcal{C}_{\infty})$. In order to simplify the design problem, we will only consider linear infinite codes. Moreover, linearity implies a lattice structure and enables the application of the Sphere Decoder (see Section 2.4).

Remark 2.1. The "pseudo-distance" $\Delta_{\min}$ is similar to the minimum Euclidean distance in the case of finite constellations carved from infinite lattices.

In order to increase reliability, we will focus on full diversity linear codes with large minimum determinant $\Delta_{\min}$.

2.3 Modulations and Full-Rate Codes

We assume that transmitted bits label some QAM or HEX *information symbols*. As basic modulation schemes we consider Q-QAM and Q-HEX constellations, where $Q = 2^q$ for some positive integer q, which offer great flexibility in terms of rates and are well suited for adaptive modulation schemes. When no outer coding is considered, the q information bits are usually mapped to information symbols by using either a Gray mapping for QAM symbols, or a mapping that mimics a Gray mapping for HEX symbols.

In the case of QAM, we assume the constellation is scaled to match $(k + 1/2) + (\ell + 1/2)i$ for $k, \ell \in \mathbb{Z}$, i.e., the minimum Euclidean distance $d_{E,\min} = 1$ and it is centered at the origin. The average energy E_s is 0.5, 1.5 and 2.5 for $Q = 4,8,16$.

Similarly, we consider Q-HEX constellations [22] carved from the translated hexagonal lattice A_2 defined by the generator matrix [11]

$$\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix},$$

which guarantees a minimum Euclidean distance $d_{E,\min} = 1$ between the modulation points. The 4-, 8- and 16-HEX are shown in Figures 2.1, 2.2, and 2.3, where the respective translation vectors (1/2,0), (1/2,0), and (1/4,0) guarantee a zero mean constellation. The bit labeling shown

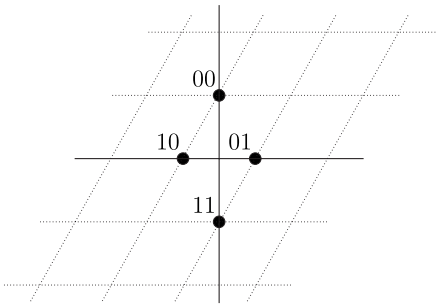

Fig. 2.1 The 4-HEX constellation.

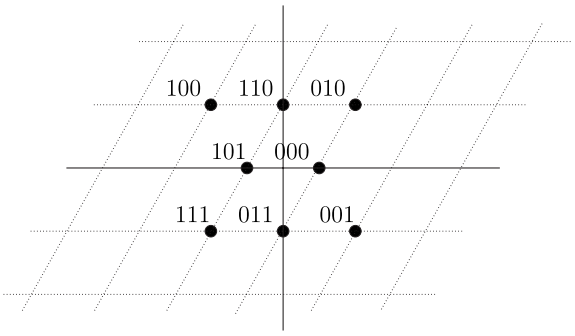

Fig. 2.2 The 8-HEX constellation.

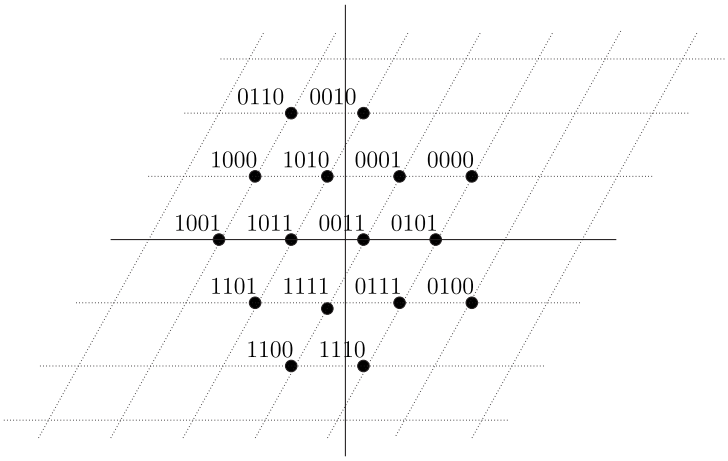

Fig. 2.3 The 16-HEX constellation.

in the figures was optimized to mimic a Gray labeling as close as possible, in order to minimize bit error probability.

The error probability performance is usually plotted as a function of $\mathsf{SNR}_b = n_t E_b/N_0$, where $E_b = E_s/q$ is the energy per bit. We have $N_0 = 2\sigma^2$, where σ^2 is the noise variance per real dimension, which can be adjusted as

$$\sigma^2 = \frac{n_t E_b}{2}\, 10^{-(\mathsf{SNR}_b)\mathrm{dB}/10}.$$

Let κ denote the number of information symbols (QAM or HEX) that are encoded in the STBC codewords. The spectral efficiency of the MIMO system will be $\eta = \kappa q/T$ bits per channel use (bpcu) or alternatively $\eta_s = \kappa/T$ symbols per channel use (spcu).

Definition 2.4. We say that a code has *full rate* when $\kappa = n_r T$.

In the next section, we will see that a linear full rate code can be decoded using a sphere decoder, whenever the codeword matrix entries are linear functions of the κ information symbols (linear encoding). Linearly encoded linear codes with $\kappa > n_r T$ will incurr in a larger ML decoding complexity.

We will focus on the case where $n_t = n_r = T = n$, then we can encode $\kappa = n^2$ information symbols, i.e., $\eta_s = n$ spcu.

In order to maximize the overall spectral efficiency, we will focus on full rate STBCs.

2.4 Decoding

We will now see how the problem of decoding linear codes can be reformulated as a lattice decoding problem, for which a Sphere Decoder can be applied [28, 60].

Consider the column-wise matrix vectorization function $\mathrm{vec}(\cdot)$ which also separates real $\Re(\cdot)$ and imaginary $\Im(\cdot)$ parts as

$$\begin{aligned}\mathrm{vec}(\mathbf{Y}) = (&\Re(y_{11}), \Im(y_{11}), \ldots, \Re(y_{n_r 1}), \Im(y_{n_r 1}), \ldots, \\ &\Re(y_{1T}), \Im(y_{1T}), \ldots, \Re(y_{n_r T}), \Im(y_{n_r T}))^T\end{aligned}$$

and the complex-to-real matrix conversion $ri(\cdot)$ which replaces each complex entry of a matrix $\mathbf{H} = (h_{ij})$ with a 2×2 real matrix

$$\begin{pmatrix} \Re(h_{ij}) & -\Im(h_{ij}) \\ \Im(h_{ij}) & \Re(h_{ij}) \end{pmatrix}.$$

The MIMO channel $\mathbf{Y} = \mathbf{HX} + \mathbf{Z}$ can be rewritten as a $2n_tT$ real vector channel $\mathbf{y} = \mathcal{H}\mathbf{x} + \mathbf{z}$, where $\mathbf{y}, \mathcal{H}, \mathbf{x}$, and $\mathbf{z}$ are given by

$$\mathrm{vec}(\mathbf{Y}) = \begin{pmatrix} ri(\mathbf{H}) & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & ri(\mathbf{H}) \end{pmatrix} \times \mathrm{vec}(\mathbf{X}) + \mathrm{vec}(\mathbf{Z}).$$

The codewords in an STBC correspond to points $\mathbf{x}$ in the $N = 2n_tT$ dimensional Euclidean space $\mathbb{R}^N$. When the STBC is a linear infinite code, the points $\mathbf{x}$ form a lattice Λ defined by some generator matrix R, so that we identify the code with the lattice

$$\mathcal{C}_\infty = \Lambda = \{\mathbf{x} = R\mathbf{u} : \mathbf{u} \in \mathbb{Z}^N\}.$$

We say that the infinite code linearly encodes the information symbols that are mapped to the integer component vector $\mathbf{u}$ in the integer component domain $\mathbb{Z}^N$.

A finite code $\mathcal{C} \subset \mathcal{C}_\infty$ corresponds to a finite constellation carved from the infinite lattice Λ

$$\begin{aligned}\mathcal{C} = \{&\mathbf{x} = R\mathbf{u} : \mathbf{u} = (u_1, \ldots, u_N), \\ &u_{2k} + iu_{2k-1} \in Q\text{-QAM for } k = 1, \ldots, N/2\}.\end{aligned}$$

Alternatively we can write $\mathcal{C} = \mathcal{B} \cap \Lambda + \mathbf{x}_0$, where $\mathcal{B}$ is the bounding region and $\mathbf{x}_0$ is an offset vector which is needed to minimize the average transmitted energy.

Let $Q\text{-QAM}^{N/2} = \mathcal{S} \cap \mathbb{Z}^N + \mathbf{u}_0$ where $\mathcal{S} = R^{-1}\mathcal{B}$ is the bounding region in the integer component domain and $\mathbf{u}_0 = R^{-1}\mathbf{x}_0$. Given the received vector $\mathbf{y} = \mathrm{vec}(\mathbf{Y})$, the ML decoder has to compute

$$\min_{\mathbf{x}\in\mathcal{C}} \|\mathbf{y} - \mathcal{H}\mathbf{x}\|^2 = \min_{\mathbf{u}\in\mathcal{S}\cap\mathbb{Z}^N+\mathbf{u}_0} \|\mathbf{y} - \mathcal{H}R\mathbf{u}\|^2 = \min_{\mathbf{u}\in\mathcal{S}\cap\mathbb{Z}^N} \|\tilde{\mathbf{y}} - \mathcal{H}R\mathbf{u}\|^2,$$

where $\tilde{\mathbf{y}} = \mathbf{y} - \mathcal{H}R\mathbf{x}_0$. This shows that the ML decoder is equivalent to a bounded lattice decoding problem which can be efficiently solved using the Sphere Decoder [13].

2.5 Constellation Shaping

In the previous section, we have seen that the MIMO system once vectorized is equivalent to a vector fading channel. The STB codewords correspond to points in a multidimensional signal space. Performance of a multidimensional constellation is partly determined by the shape of its bounding region $\mathcal{B}$. Since $\mathbb{E}[\|\mathbf{X}\|]_F^2 = \mathbb{E}[\|\mathbf{x}\|]^2 = n_t T E_s$, the codewords of $\mathcal{C}$ should be packed as efficiently as possible inside $\mathcal{B}$.

In [23], the *shaping gain* γ_s is defined relatively to a cubic bounding region for which $\gamma_s = 0\,\mathrm{dB}$. The bounding region with maximal γ_s is spherical for any dimension, and for the dimension growing to infinity it can be shown that $\gamma_s \to 1.56\,\mathrm{dB}$. On the contrary any skewed bounding region can result in a substantial shaping loss (i.e., $\gamma_s < 0\,\mathrm{dB}$) due to the higher average energy required to transmit the same number of constellation points.

Although the spherical bounding region is attractive due to its shaping gain it has the drawback that labeling the constellation

points requires a look-up table, which can be impractical for large constellations.

This forces our choice in favor of cubic constellations, which can be easily labeled and do not exhibit any shaping loss (i.e., $\gamma_s = 0\,\text{dB}$). We refer to this property as *cubic shaping*. In the following chapter (Section 3.6), we will also show that cubic shaping is related to the concept of *information lossless* STBCs.

The problem of constellation shaping can be illustrated by a toy example based on a two transmit and one receive antenna system with channel matrix $\mathbf{h} = (h_1, h_2)$ and real independent Rayleigh fading coefficients. Consider a diagonal Space–Time code with codebook [12] $\mathcal{C}$ with 2×2 diagonal matrices

$$\mathbf{X} = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix},$$

where $\mathbf{x} = (x_1, x_2)^T = \mathbf{M}(s_1, s_2)^T,\ s_1, s_2 \in \{\pm 1/2, \pm 3/2\}$ and $\mathbf{M}$ is a 2×2 matrix defining the above code. Let $\mathbf{y} = \mathbf{hX} + \mathbf{z}$ be the received vector, where $\mathbf{z}$ is the Gaussian noise vector. Then ML decoding is given by

$$\min_{\mathbf{X}\in\mathcal{C}} \|\mathbf{y} - \mathbf{hX}\|^2 = \min_{s_1,s_2\in\{\pm 1/2,\pm 3/2\}} \left\| \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} - \begin{pmatrix} h_1 & 0 \\ 0 & h_2 \end{pmatrix} \mathbf{M} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \right\|^2.$$

Performance of this code can be asymptotically estimated from the dominant term in the union bound. This term is governed by the rank of the codeword distance matrices $\mathbf{A}$ in (2.7) and, when full rank, by the minimum determinant

$$\Delta_{\min} = \min_{\mathbf{X}\neq\hat{\mathbf{X}}} \det(\mathbf{A}) = \min_{\mathbf{X}\neq\hat{\mathbf{X}}} \|x_1 - \hat{x}_1\|^2 \|x_2 - \hat{x}_2\|^2 = d^2_{p,\min},$$

where $d^2_{p,\min}$ is the square minimum *product distance* among all pairs of vectors (x_1, x_2), $(\hat{x}_1, \hat{x}_2)$. Note that $d^2_{p,\min}$ is invariant by translations of the constellation and scales with E_s^2.

Full rank diagonal STBCs correspond to full *modulation diversity* constellations (i.e., no two points have one or more coordinates in common) [43].

Figures 2.4(a), 2.4(b), and 2.5 show the transmitted signal set corresponding to different codes defined by the matrices $\mathbf{M}$. In general the receiver will see a compressed or expanded signal set on the x- and y-axis depending on the fading coefficients h_1 and h_2.

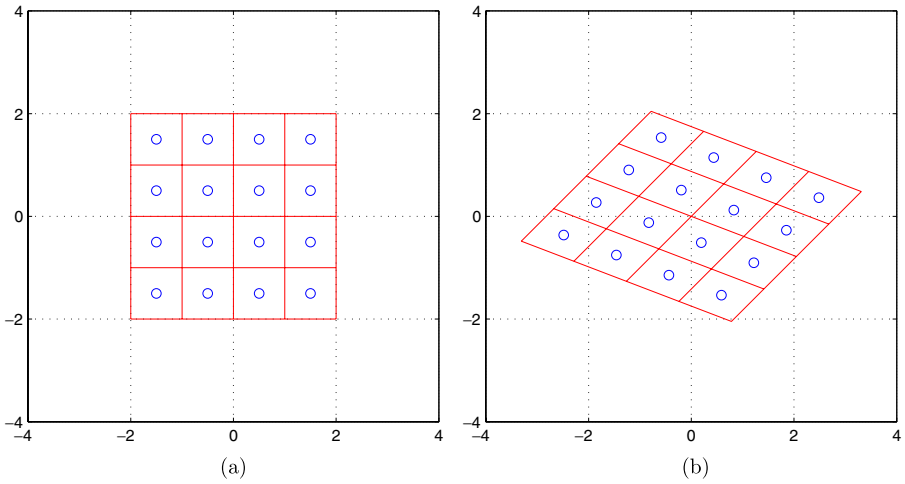

Fig. 2.4 (a) On the left, the 16-QAM constellation with $d^2_{p,\min} = 0$, $d_{E,\min} = 1$, and $E_s = 2.5$, (b) on the right, an algebraic constellation with diversity, $d^2_{p,\min} = 4/25$, $d_{E,\min} = 0.8944$, and $E_s = 12.5$.

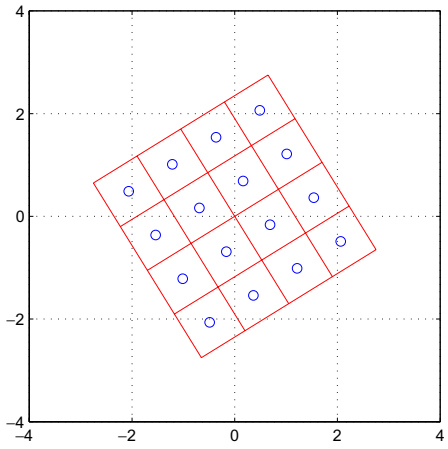

Fig. 2.5 Algebraically rotated 16-QAM constellation with diversity, $d^2_{p,\min} = 1/5$, $d_{E,\min} = 1$, and $E_s = 2.5$.

We will use these three codes to illustrate the trade-off among diversity, coding gain and constellation shaping. In the following, $d_{E,\min}$ will denote the *minimum Euclidean distance*.

The 16-QAM constellation in Figure 2.4(a) with $\mathbf{M}$ the identity matrix and $d_{E,\min} = 1$ has an average energy of $E_s = 2.5$, but due to the lack of diversity cannot deliver the full information if one of the two channels is completely faded ($h_i \approx 0$). In this case the constellation points seen by the receiver collapse onto each other giving rise to systematic errors even in the presence of very little noise.

If we consider the algebraic constellation of Figure 2.4(b) with $\mathbf{M}$ given by the canonical embedding of $\mathbb{Q}(\sqrt{5})$ (see Section 4.4.1 and [43])

$$\mathbf{M} = c \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}$$

we get the full modulation diversity. The coefficient c is used for normalization purposes. Setting $c = 1/\sqrt{2}$ we have $d_{E,\min} = 1$ but this requires an average energy of $E_s = 3.125$ (25% more); alternatively with $c = \sqrt{2/5}$ we have the same energy $E_s = 2.5$ but $d_{E,\min} = 0.8944$. The same modulation diversity can be obtained by an algebraic rotation [43], which also preserves the original average energy $E_s = 2.5$ without sacrificing $d_{E,\min}$ (see Figure 2.5). The corresponding matrix is given by

$$\mathbf{M} = \frac{1}{\sqrt{5}} \begin{pmatrix} \sqrt{2 + \frac{1+\sqrt{5}}{2}} & 0 \\ 0 & \sqrt{2 + \frac{1-\sqrt{5}}{2}} \end{pmatrix} \begin{pmatrix} 1 & \frac{-1+\sqrt{5}}{2} \\ 1 & \frac{-1-\sqrt{5}}{2} \end{pmatrix}.$$

Intuitively, the diagonal matrix is designed to skew the constellation in Figure 2.4(b) into the cubic shaped one in Figure 2.5 without loosing the full diversity (see [43]).

Considering $\Delta_{\min} = d^2_{p,\min}$, the 16-QAM constellation in Figure 2.4(b) has $d^2_{p,\min} = 0$ since it is not full rank, while the other two exhibit a positive $d^2_{p,\min}$. This can be estimated using the infinite lattice constellation and (2.13). Using the theory of algebraic and ideal lattices [3] we find $d^2_{p,\min} = 4/25$ for the algebraic lattice constellation and $d^2_{p,\min} = 1/5$ for the algebraically rotated 16-QAM [43].

The performance of the codeword error probability for the three codes is shown in Figure 2.6. It is clear that the 16-QAM has a slope

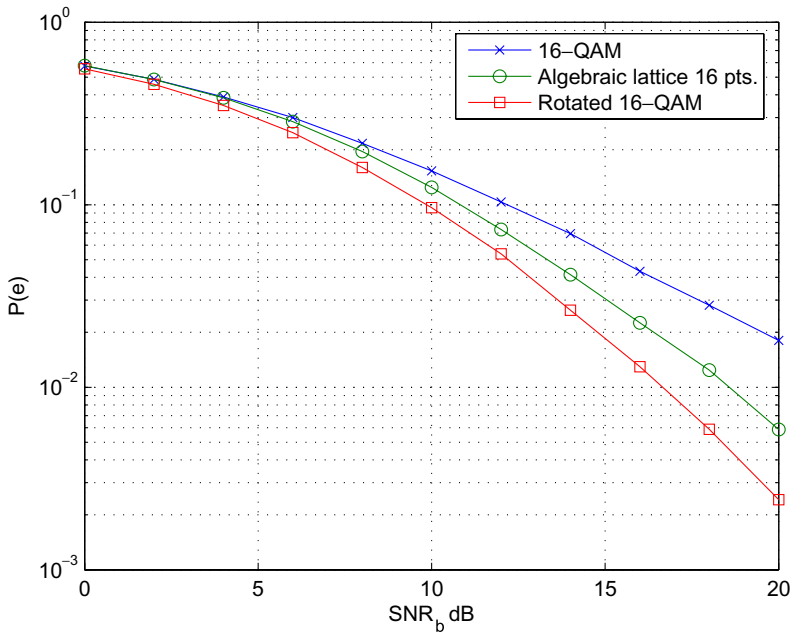

Fig. 2.6 Comparison of the codeword error probability for the three codes.

corresponding to a diversity one, while the other two have diversity two. The rotated 16-QAM exhibits a better performance thanks to the higher value of $\Delta_{\min}$.

In order to save on the average transmitted energy, we will require cubic shaping of the STBCs.

Raj Kumar and Caire [46] recently proposed a nonlinear mapping encoder which can result in some shaping gain of the transmitted constellation. This can outperform the above choice of cubic shaping at the price of some additional complexity at the encoder.

Let us conclude this section by a few remarks, about another code property required for the design, called *non-vanishing determinant* (NVD).

Adaptive modulation schemes require the transmission of different size constellations. It is therefore important that the coding gain of the code does not depend on the constellation size. In particular, we

are interested in infinite codes with nonzero $\Delta_{\min}$. We call this the *non-vanishing determinant* property. This property was first proposed in [6]. Previous STBC constructions proposed in the literature had a minimum determinant decreasing with the constellation size and eventually vanishing for the infinite code.

NVD codes are also useful in bandwidth efficient concatenated coding schemes, where the outer code redundancy can be absorbed by a constellation expansion. A vanishing determinant can drastically reduce the overall coding gain [32].

The NVD property is a necessary and sufficient condition for an ST coding scheme to achieve the diversity-multiplexing trade-off [20]. In the following chapter we will show that

In order to achieve the diversity-multiplexing trade-off, we will focus on NVD linear codes.

Let us conclude this chapter by briefly summarizing what will be our target design criteria: we aim at designing linear Space–Time block codes with $n_t = n_r = T$, that are fully-diverse with large minimum determinant, to increase the system reliability. To maximize spectral efficiency, we will focus on full rate codes, and cubic shaping is needed to save on the average transmitted energy. Finally, we require the codes to have a non-vanishing determinant.

In the next chapter, we will look at the code design from an information theoretic point of view.

3

An Information Theoretic Perspective

In this chapter, we will see that two main features are important, to ensure the good performance of a coding scheme from an information theoretic point of view: (i) reaching the *diversity-multiplexing gain trade-off* and (ii) using *information lossless* codes. We will see that both these properties will correspond to other properties already required. Namely, the non-vanishing determinant property will be shown to be a sufficient condition to reach the diversity-multiplexing gain, and the cubic shaping will give information lossless codes.[1]

Historically, the first 2×2 Space–Time code to achieve the diversity-multiplexing gain trade-off has been found by Yao and Wornell in [63], where they show that for a 2×2 code, having a minimum determinant bounded away from zero when the constellation size increases with SNR is a sufficient condition to reach the trade-off. This notion later on appeared to be similar to the non-vanishing determinant property introduced independently by Belfiore and Rekaya [6]. In [20], the non-vanishing determinant property is shown to be in general a sufficient condition for division algebra codes to reach the trade-off.

[1] Part of this chapter is inspired by the book [59].

3.1 Mutual Information of a Gaussian MIMO Channel

Let us start by considering a MIMO Gaussian channel characterized by a *fixed* $n_r \times n_t$ complex matrix $\mathbf{H} = [h_{ij}]$. Recall that each term h_{ij} is the complex attenuation factor between receive antenna i and transmit antenna j. At each symbol time, the received signal is the n_r-dimensional vector

$$\mathbf{y} = \mathbf{H}_{n_r \times n_t}\mathbf{x} + \mathbf{z}, \tag{3.1}$$

where $\mathbf{x}$ is the transmitted vector of dimension n_t and $\mathbf{z}$, which represents the noise, is a Gaussian vector with n_r *i.i.d.* components.

Note that this is a particular realization of the original channel (2.1), where the coherence time is $T = 1$, and the channel matrix is fixed.

Theorem 3.1 [58]. Assume that the vector $\mathbf{x}$ has circularly complex Gaussian distributed components and $\mathbf{H}$ is deterministic. Then, the expression of the mutual information is

$$I(\mathbf{x};\mathbf{y}|\mathbf{H}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{1}{\sigma^2}\mathbf{H}\mathbf{Q}\mathbf{H}^\dagger\right), \tag{3.2}$$

where $\mathbf{I}_{n_r}$ is the identity matrix with dimension n_r, σ^2 is the variance of each real component of the noise $\mathbf{z}$ and $\mathbf{Q}$ is the covariance matrix of $\mathbf{x}$,

$$\mathbf{Q} = \mathbb{E}[\mathbf{x}\mathbf{x}^\dagger]. \tag{3.3}$$

When the transmitter knows perfectly $\mathbf{H}$, then it can optimize mutual information with *water-filling* [58, 59] which achieves

$$\max_{\mathbf{Q}, \mathrm{Tr}(\mathbf{Q}) \leq P_{\mathbf{x}}} I(\mathbf{x}, \mathbf{y}), \tag{3.4}$$

where $P_{\mathbf{x}}$ is the maximum power available at the transmitter.

We now consider the case where the receiver knows the channel, but this channel is random. Here, we follow Telatar in [58, p. 22] who conjectures that when the channel matrix is random, non-ergodic, then, in the high SNR region, the optimal covariance matrix for the source is

$\mathbf{Q}_{\text{opt}} = (P_{\mathbf{x}}/n_t) \cdot \mathbf{I}_{n_t}$. By using this value of $\mathbf{Q}_{\text{opt}}$, we deduce the value of mutual information

$$I(\mathbf{x};\mathbf{y}) = \log_2 \det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^\dagger\right), \tag{3.5}$$

which corresponds to a strategy where the source transmits the signal *isotropically* (that is, its probability density function is invariant to multiplication by a unitary matrix).

3.2 The Outage Probability

The *outage probability* is a key concept in wireless communications. If we assume that the channel is not fixed but can be represented by a random matrix $\mathbf{H}$, then the mutual information given by (3.5) becomes a random variable which is denoted by $C(\mathbf{H})$. When we consider a quasi-static channel, we assume that the channel matrix remains constant during the transmission of a codeword, say of length T, as in (2.1):

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t}\mathbf{X}_{n_t \times T} + \mathbf{Z}_{n_r \times T}.$$

Whenever the data rate R is lower than $C(\mathbf{H})$, then it is possible to find a code which achieves an arbitrarily low error probability. But when $C(\mathbf{H}) < R$, then we say that the channel is in outage. We define the outage probability as

---

Definition 3.1. The *outage probability* of a MIMO channel is

$$P_{\text{out}}^{\text{MIMO}}(R) = \min_{\mathbf{Q}, \text{Tr}(\mathbf{Q}) \leq P_{\mathbf{x}}} \Pr\left\{\log_2 \det\left(\mathbf{I}_{n_r} + \mathbf{H}\mathbf{Q}\mathbf{H}^\dagger\right) < R\right\}. \tag{3.6}$$

The optimal covariance matrix depends on the SNR and on the rate R. The choice $\mathbf{Q} = (P_{\mathbf{x}}/n_t) \cdot \mathbf{I}_{n_t}$ is often used as it is a good approximation of the optimal covariance matrix. Since we are interested in the SNR exponent of the outage which is the same in both cases, we will use a definition of the outage probability when using an *i.i.d.* source,

$$P_{\text{out}}^{\text{MIMO,i.i.d}}(R) = \Pr\left\{\log_2 \det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^\dagger\right) < R\right\}. \tag{3.7}$$

Definition 3.2. The *diversity order of a channel* is defined as the negative of the slope of the outage probability when plotted in a log–log scale versus SNR.

Similarly to this definition of the channel diversity, we can define the diversity order of a coding scheme,

Definition 3.3. The *diversity order of a coding scheme* is defined as the negative of the slope of the word error probability when plotted in a log–log scale versus SNR.

We note that the diversity order of the channel gives the maximum diversity gain achievable by any coding scheme operating over such channel.

3.2.1 The SISO Case

We consider the case where we have only one transmit and one receive antenna (Single Input Single Output), that is

$$y = hx + z.$$

Let h be a zero-mean Gaussian random variable with variance 1. The fading of the channel is thus assumed to be Rayleigh distributed, which means that $|h|^2$ is exponentially distributed. The outage probability is given by

$$P_{\text{out}}^{\text{SISO}}(R) = \Pr\left\{\log_2\left(1 + \mathsf{SNR}|h|^2\right) < R\right\} = \Pr\left\{|h|^2 < \frac{2^R - 1}{\mathsf{SNR}}\right\}.$$

We get

$$P_{\text{out}}^{\text{SISO}}(R) = 1 - \exp\left(-\frac{\left(2^R - 1\right)}{\mathsf{SNR}}\right)$$

which gives at high SNR,

$$P_{\text{out}}^{\text{SISO}}(R) \approx \frac{2^R - 1}{\mathsf{SNR}}. \tag{3.8}$$

We remark that the outage probability asymptotically decays as $1/\mathsf{SNR}$ for a fixed rate. This channel has diversity order one.

3.2.2 Receive Diversity: The SIMO Case

In the Single Input Multiple Output case (SIMO), the receiver is assumed to be equipped with an antenna array in order to increase the spatial diversity order of the channel. Here, the transmitted vector is in fact a scalar and the channel is a column vector $\mathbf{h}$ with n_t components,

$$\mathbf{y} = \mathbf{h}_{n_t} x + \mathbf{z}.$$

The outage probability for the SIMO case is

$$P_{\text{out}}^{\text{SIMO}}(R) = \Pr\{\log_2(1 + \mathsf{SNR}\,\|\mathbf{h}\|^2) < R\}, \tag{3.9}$$

which yields

$$P_{\text{out}}^{\text{SIMO}}(R) = \Pr\left\{\|\mathbf{h}\|^2 < \frac{2^R - 1}{\mathsf{SNR}}\right\}. \tag{3.10}$$

If we suppose that the channel coefficients are Gaussian zero-mean and spatially uncorrelated, then $\|\mathbf{h}\|^2$ is a χ-square distributed random variable with $2n_t$ degrees of freedom. Its probability density function (*pdf*) is

$$p_{\|\mathbf{h}\|^2}(x) = \frac{1}{(n_r - 1)!} x^{n_r - 1} e^{-x} \mathbf{1}_{\mathbb{R}^+}, \tag{3.11}$$

where $\mathbf{1}_{\mathcal{S}}$ is the indicator function of the set $\mathcal{S}$. Let ϵ be an arbitrarily small positive real number. Then, by approximating e^{-x} by 1 for x small, we get

$$\Pr\{\|\mathbf{h}\|^2 < \epsilon\} \approx \frac{1}{n_r!} \epsilon^{n_r}. \tag{3.12}$$

By applying (3.12) to the expression of the outage probability at high SNR, we get

$$P_{\text{out}}^{\text{SIMO}}(R) \approx \frac{\left(2^R - 1\right)^{n_r}}{n_r! \mathsf{SNR}^{n_r}}. \tag{3.13}$$

Now, the outage probability asymptotically decays as $1/\mathsf{SNR}^{n_r}$, hence n_r is the diversity order of this channel.

3.2.3 Transmit Diversity: The MISO Case

In the Multiple Input Single Output (MISO) case

$$y = \mathbf{h}_{1\times n_t}\mathbf{x} + z$$

the channel is a row vector $\mathbf{h}$ with n_t components, which are assumed to be *i.i.d.* zero-mean Gaussian. The outage probability for the MISO case is

$$P_{\text{out}}^{\text{MISO}}(R) = \Pr\left\{\log_2\left(1 + \frac{\mathsf{SNR}}{n_t}\|\mathbf{h}\|^2\right) < R\right\}, \tag{3.14}$$

which yields

$$P_{\text{out}}^{\text{MISO}}(R) = \Pr\left\{\|\mathbf{h}\|^2 < \frac{n_t\left(2^R - 1\right)}{\mathsf{SNR}}\right\}. \tag{3.15}$$

The same calculation as for the SIMO case yields

$$P_{\text{out}}^{\text{MISO}}(R) \approx \frac{n_t^{n_t}\left(2^R - 1\right)^{n_t}}{n_t!\mathsf{SNR}^{n_t}} \tag{3.16}$$

enlightening a transmit diversity order equal to n_t.

3.2.4 The MIMO Case

The calculation of the outage probability for the MIMO case is more difficult than for the previous above cases, but we can start by intuitively explaining the behavior of the SNR exponent. We follow the method developed in [59]. In the MIMO case, the channel matrix $\mathbf{H}$ is a $n_r \times n_t$ matrix with zero-mean Gaussian i.i.d. components. Let $q = \min\{n_t, n_r\}$. Then the outage probability is given by

$$P_{\text{out}}^{\text{MIMO}}(R) = \Pr\left\{\sum_{i=1}^{q}\log_2\left(1 + \frac{\mathsf{SNR}}{n_t}\lambda_i^2\right) < R\right\}, \tag{3.17}$$

where λ_is are the singular values of the matrix $\mathbf{H}$. The MIMO channel exhibits q modes of transmission, each corresponding to an instantaneous SNR equal to $\left(\mathsf{SNR}\lambda_i^2\right)/n_t$. How effective each mode is depends on how large the instantaneous SNR is. For large values of SNR, we say that mode i is *effective* if $\left(\mathsf{SNR}\lambda_i^2\right)/n_t$ is of order SNR and *not effective*

if $\left(\mathsf{SNR}\lambda_i^2\right)/n_t$ is of order 1 or less. Consider (3.17), there is an *outage event* when none of the modes are effective. That means that all λ_i^2 are of order $1/\mathsf{SNR}$ or less. Remark that

$$\sum_{i=1}^{q} \lambda_i^2 = \mathrm{Tr}(\mathbf{H}\mathbf{H}^\dagger) = \sum_{i,j} |h_{ij}|^2 .$$

So there is an outage event when each $|h_{ij}|^2$ is of order $1/\mathsf{SNR}$ or less. Since all $|h_{ij}|^2$ are independent and $\Pr\{|h_{ij}|^2 < 1/\mathsf{SNR}\} \approx 1/\mathsf{SNR}$, the outage probability is

$$P_{\mathrm{out}}^{\mathrm{MIMO}}(R) = \Pr\left\{ \bigcap_{i,j} \left(|h_{ij}|^2 < 1/\mathsf{SNR} \right) \right\} = O\left(\frac{1}{\mathsf{SNR}^{n_t n_r}} \right). \quad (3.18)$$

The channel diversity order obtained from the outage probability calculation in the MIMO case is $n_r n_t$.

3.3 Diversity-Multiplexing Gain Trade-off of MIMO Channels

This section is mainly inspired by [59] and [64]. In the following, DMT will stand for Diversity-Multiplexing Trade-off.

3.3.1 Diversity and Multiplexing Gain

For the scalar Gaussian channel,

$$y' = hx' + z',\ h \text{ fixed},$$

or equivalently

$$y = x + z,$$

there is a trade-off between the data rate that can be transmitted and the performance that we can expect. Since the capacity of the scalar Gaussian channel is given by

$$C = \log_2(1 + \mathsf{SNR}) \quad (3.19)$$

expressed in bits **p**er **c**hannel **u**se (or bits pcu), we have a natural way of characterizing the rate/performance trade-off. The rate is represented

by the capacity when performance is represented by the minimum necessary SNR to achieve the rate C. Asymptotically ($\mathsf{SNR} \to \infty$), we see that in order to have 1 bit pcu more, we need 3 dB more.

Now, consider the case of a parallel (vector) Gaussian channel where the transmitter does not know the values of SNRs as depicted in Figure 3.1. As there is no channel side information at the transmitter, then the transmitter shares the total available power among all channels. Thus when the noise power decreases by 3 dB, then all SNR_is increase by 3 dB giving rise to an increased data rate equal to 1 bit per channel and pcu, which gives an increase of q bits pcu. So, asymptotically, the capacity of the parallel Gaussian channel varies as $q \log_2 \mathsf{SNR}$ bits pcu.

A MIMO Rayleigh fading channel, when the transmitter does not know the channel matrix $\mathbf{H}$, has an instantaneous capacity

$$C(\mathbf{H}) = \sum_{i=1}^{q} \log_2 \left(1 + \frac{\mathsf{SNR}}{n_t} \lambda_i^2\right), \tag{3.20}$$

where λ_is are the singular values of $\mathbf{H} = \mathbf{H}_{n_t \times n_r}$. This channel can be viewed as a vector Gaussian channel with $\mathsf{SNR}_i = \mathsf{SNR}\lambda_i^2/n_t$. Like the Gaussian vector channel, the MIMO channel exhibits q transmission modes where $q = \min\{n_t, n_r\}$.

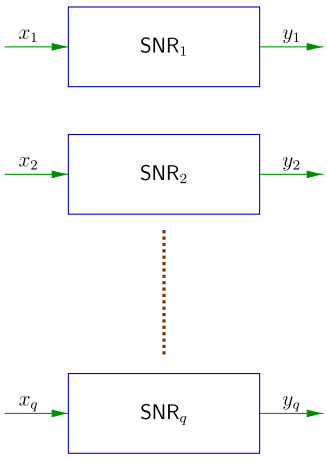

Fig. 3.1 Compound Gaussian channel.

Since the MIMO channel has thus $q = \min\{n_t, n_r\}$ degrees of freedom, this means that we can at most transmit $\eta_s = q$ symbols per channel use reliably.

Note furthermore that these q modes are random since λ_is are random. So, $C(\mathbf{H})$ cannot represent some data rate anymore. Performance cannot be represented by the SNR either, since the relationships (3.20) are much more complicated than in the Gaussian case.

A good performance criterion is the outage probability. But this probability depends on the rate and on the SNR. The analysis of what happens in the SISO, SIMO, and MISO cases will provide some understanding on this problem. In order to eliminate one variable among three (P_{out}, SNR, and R), we examine the behavior of P_{out} at high SNR and force R to vary as if the channel was equivalent to r parallel subchannels, namely

$$R = r \log_2 \mathsf{SNR}.$$

The diversity order d is the exponent of $1/\mathsf{SNR}$ in the asymptotic expression of P_{out} and we define the *multiplexing gain* r as being the number of subchannels of the MIMO channel asymptotically viewed as a parallel channel. More formally, we have the following definitions given by the expression of the outage probability.

Definition 3.4. A *diversity gain*[2] $d^*(r)$ is achieved at multiplexing gain r if

$$-\lim_{\mathsf{SNR}\to+\infty} \frac{\log P_{\text{out}}\left(r \log_2 \mathsf{SNR}\right)}{\log \mathsf{SNR}} = d^*(r). \tag{3.21}$$

3.3.2 The SISO Case

By writing that $R = r \log_2 \mathsf{SNR}$ in (3.8), we get

$$P_{\text{out}}^{\text{SISO}}(r \log_2 \mathsf{SNR}) \approx \frac{\mathsf{SNR}^r}{\mathsf{SNR}}.$$

[2] Note that it is a channel diversity gain (see Definition 3.2).

Hence, by Definition 3.4, we have

$$d^*_{\mathrm{SISO}}(r) = 1 - r \tag{3.22}$$

for $0 \leq r \leq 1$.

3.3.3 The SIMO/MISO Case

For the SIMO case, (3.13) with $R = r \log_2 \mathsf{SNR}$ gives

$$P^{\mathrm{SIMO}}_{\mathrm{out}}(r \log_2 \mathsf{SNR}) \approx \frac{\mathsf{SNR}^{r \cdot n_r}}{n_r! \mathsf{SNR}^{n_r}}.$$

Thus

$$d^*_{\mathrm{SIMO}}(r) = n_r (1 - r) \tag{3.23}$$

for $0 \leq r \leq 1$. The same calculation for the MISO case gives

$$d^*_{\mathrm{MISO}}(r) = n_t (1 - r). \tag{3.24}$$

3.3.4 The MIMO Case

The general case is much more difficult to obtain. The main result is the following theorem which is proven in [64].

Theorem 3.2. The diversity-multiplexing gain trade-off of a MIMO $n_t \times n_r$ *i.i.d.* Rayleigh fading channel is a piecewise linear curve joining the points

$$\begin{pmatrix} k \\ (n_t - k)(n_r - k) \end{pmatrix}$$

with $k \in \{0, 1, \ldots, q\}$ and $q = \min\{n_t, n_r\}$.

The proof is difficult but we can give some intuitive sketch of the proof. It generalizes in fact the result of (3.18). We calculate, for high values of SNR, with $R = r \log_2 \mathsf{SNR}$,

$$P^{\mathrm{MIMO}}_{\mathrm{out}}(R) = \Pr\left\{ \sum_{i=1}^{q} \log_2 \left(1 + \frac{\mathsf{SNR}}{n_t} \lambda_i^2 \right) < r \log_2 \mathsf{SNR} \right\}. \tag{3.25}$$

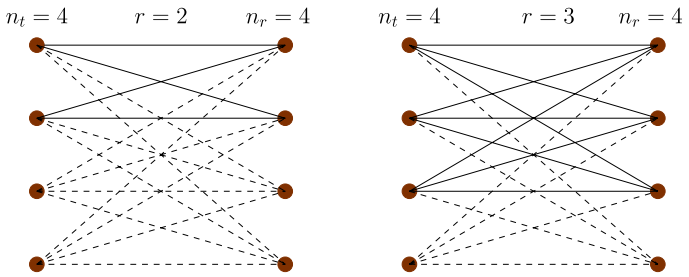

Fig. 3.2 Graph of a MIMO channel with r data flows.

Fix r being a positive integer. At high SNR, the outage region is the region where r of the modes are effective and the other ones not. That means that r singular values of $\mathbf{H}$ are of order 1 and the other ones of order $1/\mathsf{SNR}$ or less. So it implies that $\mathbf{H}$ is close to a rank r matrix. For the case $r = 0$, the outage event is when $\mathbf{H}$ is close to a rank 0 matrix. So, by Equation (3.18), the diversity gain is $d^*_{\text{MIMO}}(0) = n_t n_r$. Another interpretation is given in Figure 3.2. If r is an integer, then it can be viewed as some "*network flow*" of the graph, and $d(r)$ becomes the minimum "*cost*" to limit the network flow to r. In particular, $d(0)$ is the "*disconnection cost.*" For example, if $r = 2$, then it remains four edges that one needs to cut in order to keep two data flows. Four is equal to $d(2)$ for a $n_t = 4, n_r = 4$ MIMO channel. With this interpretation, we can also deduce that $d_{n_t,n_r}(r) = d_{n_t-r,n_r-r}(0)$ when r is an integer.

For the general case, let

$$\mathcal{O}(r,\mathsf{SNR}) = \left\{ \mathbf{H} \mid \sum_{k=1}^{q} \log_2(1 + \mathsf{SNR}\lambda_k) < r \log_2 \mathsf{SNR} \right\} \tag{3.26}$$

be the outage region of the channel. We get[3]

$$\mathcal{O}(r,\mathsf{SNR}) = \left\{ \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_q) : \sum_{k=1}^{q} (1 - \alpha_k)^+ < r \right\}, \tag{3.27}$$

where $\lambda_k \doteq \mathsf{SNR}^{-\alpha_k}$. It has been shown [64] that

$$p_{\boldsymbol{\alpha}}(\boldsymbol{\alpha}) \doteq \mathsf{SNR}^{-\varepsilon_{\boldsymbol{\alpha}}} \text{ where } \varepsilon_{\boldsymbol{\alpha}} = \sum_{k=1}^{q} (2k - 1 + |n_t - n_r|)\,\alpha_k$$

[3] The notation $(x)^+$ is for $\max(0, x)$.

and $x \doteq y$ means that

$$\lim_{\mathsf{SNR}\to\infty} \frac{\log x}{\log \mathsf{SNR}} = \lim_{\mathsf{SNR}\to\infty} \frac{\log y}{\log \mathsf{SNR}}.$$

In fact, since we are interested by the exponent of SNR, this "exponential" equality is enough to derive the DMT of the channel. So,

$$\begin{aligned} P_{\text{out}}^{\text{MIMO}}(r \log_2 \mathsf{SNR}) &= \int_{\mathcal{O}} p_{\boldsymbol{\alpha}}(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\ &\doteq \int_{\mathcal{O}} \mathsf{SNR}^{-\epsilon_{\boldsymbol{\alpha}}} d\boldsymbol{\alpha} \doteq \mathsf{SNR}^{-\inf_{\mathcal{O}} \epsilon_{\boldsymbol{\alpha}}}, \end{aligned} \quad (3.28)$$

which gives

$$d^*(r) = \inf_{\mathcal{O}} \epsilon_{\boldsymbol{\alpha}} = \min_{\mathcal{O}} \epsilon_{\boldsymbol{\alpha}}$$

that can be solved via a linear programming approach in order to give the result of Theorem 3.2.

3.4 Trade-off Achieving Codes

Similarly to the definition of the diversity order, we can define the DMT of the channel and the DMT of a coding scheme. The first one has already been defined. We give here the definition of the second one,

---

Definition 3.5. A *diversity gain* $d^*(r)$ is achieved at multiplexing gain r, for a given coding scheme, if

$$-\lim_{\mathsf{SNR}\to+\infty} \frac{\log P(e)\,(r \log_2 \mathsf{SNR})}{\log \mathsf{SNR}} = d^*(r), \quad (3.29)$$

where $P(e)$ is the word error rate of the coding scheme used on the given channel. This is the DMT of the coding scheme.

A trade-off achieving code is a code whose DMT is equal to the channel DMT, which means that the DMT calculated from the codeword error probability of the scheme is equal to the DMT of the channel

(calculated from the outage probability). Zheng and Tse [64] proved the achievability of the DMT of the channel by using a family of random Gaussian codes if the code length satisfies

$$T \geq n_t + n_r - 1. \tag{3.30}$$

A second family of DMT-achieving codes, named LAST codes, has then been proposed in [17]. The main advantage of these codes compared to the Gaussian ones is that they are much more easily decodable. However, the constraint on the delay (see (3.30)) remains the same. This constraint has been relaxed in [20] where $T \geq n_t + n_r - 1$ has been extended to $T \geq n_t$.

The concept of *approximately universal codes* that are able to achieve the diversity multiplexing gain trade-off (DMT) of the channel was introduced in [57].

Definition 3.6. An *approximately universal code* (in fact a family of codes with varying rates) is a code which is able to achieve an arbitrarily small error probability in the high SNR regime when the channel is not in outage or, equivalently, (see [59, Chapter 9]) a coded scheme which is in deep fading only when the channel itself is in outage.

This is sufficient to achieve the DMT of the outage probability (see Definition 3.4). In this work, we do not often use the concept of approximately universal codes even if all the codes that we will construct are in fact approximately universal.

As it has already been noticed, a single coding scheme is not enough to achieve the DMT. As we must rewrite the spectral efficiency as $R = r \log_2 \mathsf{SNR}$, that means that we need a family of coding schemes with increasing spectral efficiencies. We explain this concept below by starting with some simple examples.

3.4.1 SISO Channel: QAM is DMT Achieving

Let the channel be a scalar channel with $\mathbf{H} = h$, where h is a Gaussian normalized complex random variable. The energy of a QAM

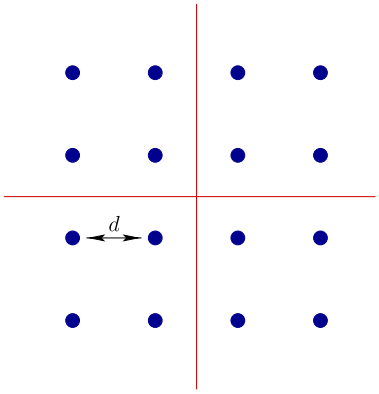

Fig. 3.3 16-QAM constellation.

constellation carrying R bits (pcu) is

$$E_{\mathrm{QAM}}(R) = \frac{d^2\left(2^R - 1\right)}{6} \tag{3.31}$$

for a fixed minimum squared Euclidean distance equal to d^2 (see Figure 3.3). For a fixed channel coefficient h, we get the expression of the symbol error probability

$$P^{\mathrm{QAM}}(e|h) = 4\mathcal{Q}\left(\sqrt{\frac{6\mathsf{SNR}}{(2^R-1)}\,|h|^2}\right), \tag{3.32}$$

where $\mathcal{Q}(x)$ is the error function, $\mathcal{Q}(x) \triangleq \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} du$. At high SNR, we replace R with $r\log_2\mathsf{SNR}$ and average over $|h|^2$ which is exponentially distributed. So, as it was stated above, the spectral efficiency of the scheme goes to infinity with the SNR. By setting $R = r\log_2\mathsf{SNR}$, we get an approximation of the average error probability in the high SNR region,

$$P^{\mathrm{QAM}}(e) \approx \mathsf{SNR}^{-(1-r)}.$$

The exponent of SNR is the same as the outage probability one. So, QAM is DMT achieving. The same conclusion applies for HEX modulation (see Section 2.3).

3.4.2 SIMO Channel: QAM is DMT Achieving

By using a Maximum Ratio Combiner, we get

$$P^{\mathrm{QAM}}(e|h) = 4\mathcal{Q}\left(\sqrt{\frac{6\mathsf{SNR}}{(2^R-1)}\sum_{i=1}^{n_r}|h_i|^2}\right). \tag{3.33}$$

As for the SISO case, at high SNR, we replace R with $r\log_2\mathsf{SNR}$ and average over the vector $(h_1, h_2, \ldots, h_{n_r})$. By setting $R = r\log_2\mathsf{SNR}$, we get an approximation of the average error probability in the high SNR region,

$$P^{\mathrm{QAM}}(e) \approx \mathsf{SNR}^{-n_r(1-r)}.$$

The exponent of SNR is still equal to the DMT of the SIMO channel so that we can state that QAM modulation achieves the DMT.

3.4.3 MISO Channel: The Alamouti Code

We will show now that the Alamouti code [1] with QAM symbols is DMT achieving for $n_r = 1$ receive and $n_t = 2$ transmit antennas.

An Alamouti codeword is of the form:

$$\mathbf{X} = \begin{bmatrix} s_1 & -\overline{s_2} \\ s_2 & \overline{s_1} \end{bmatrix},$$

where s_1, s_2 are the information symbols and $\bar{}$ denotes the complex conjugation. Note that the Alamouti code is fully diverse since

$$\det(\mathbf{X}) = |s_1|^2 + |s_2|^2 > 0,$$

for any $s_1, s_2 \in \mathbb{C}$ nonzero. The Alamouti code became popular thanks to its excellent performance. Alamouti designed it to be fully diverse, and when the diversity-multiplexing has been understood, it appeared that the Alamouti code is actually DMT achieving for the MISO case, which we will explain now.

When using the Alamouti code, the received signal

$$[y_1\ y_2] = [h_1\ h_2]\begin{bmatrix} s_1 & -\overline{s_2} \\ s_2 & \overline{s_1} \end{bmatrix} + [z_1\ z_2]$$

can be written as

$$\begin{bmatrix} y_1 \\ \overline{y_2} \end{bmatrix} = \begin{bmatrix} h_1 & h_2 \\ \overline{h_2} & -\overline{h_1} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ \overline{z_2} \end{bmatrix}. \tag{3.34}$$

The two columns of the matrix $\mathfrak{H}$ containing the channel coefficients are orthogonal and have the same magnitude, so that, by multiplying the received vector in (3.34) by $\mathfrak{H}^\dagger$, we get a new vector with components r_i with,

$$\begin{cases} r_1 = \left(|h_1|^2 + |h_2|^2\right) s_1 + w_1 \\ r_2 = \left(|h_1|^2 + |h_2|^2\right) s_2 + w_2, \end{cases} \tag{3.35}$$

where the noise terms w_1 and w_2 are i.i.d. We remark that, for each symbol s_i, the channel is now equivalent to a SIMO channel. So, the error probability is approximately given, in the high SNR region, by

$$P^{\text{Alamouti}}(e) \approx \mathsf{SNR}^{-2(1-r)}.$$

Thus the Alamouti code achieves the DMT of a MISO channel with $n_t = 2$ transmit antennas.

3.4.4 MIMO Channel: Approximately Universal Codes

For a MIMO channel, recall (see (2.5)) that the pairwise error probability of detecting the codeword $\mathbf{X}_2$ when the codeword $\mathbf{X}_1 \neq \mathbf{X}_2$ has been sent, conditioned on a MIMO channel realization $\mathbf{H}$ is given by

$$\Pr(\mathbf{X}_1 \to \mathbf{X}_2 | \mathbf{H}) = \mathcal{Q}\left(\frac{\|\mathbf{H}(\mathbf{X}_1 - \mathbf{X}_2)\|}{\sqrt{2N_0}}\right). \tag{3.36}$$

Now, the main idea to derive a design criterion for approximately universal codes consists of saying that:

(1) The MIMO channel has $q = \min\{n_t, n_r\}$ eigen directions.
(2) Remark in (3.36) that the worst-case channel not in outage aligns itself in the weakest directions of the codeword difference matrix, i.e., the directions corresponding to the smallest singular values of the codeword difference.

(3) In the high SNR region, it is equivalent to maximize the product distance

$$|\lambda_1 \cdot \lambda_2 \cdots \lambda_q|,$$

where $\lambda_1, \ldots, \lambda_q$ are the q smallest singular values of the difference matrix $\mathbf{X_1} - \mathbf{X_2}$ (when $n_t \leq n_r$, they are all the singular values of $\mathbf{X_1} - \mathbf{X_2}$).

It has been shown in [57] that a sufficient condition to have approximately universal codes is that for all pairs of distinct codewords,

$$|\lambda_1 \cdot \lambda_2 \cdots \lambda_q|^{\frac{2}{q}} > \frac{c}{q2^R}, \tag{3.37}$$

where c is some positive constant.

Moreover, a code satisfying (3.37) for an $n_t \times n_t$ MIMO channel is also approximately universal for an $n_t \times n_r$ channel for every value of n_r, the number of receive antennas, which can be stated as

---

Proposition 3.3. An approximately universal Space–Time code for a MIMO $n_t \times n_t$ channel is approximately universal for a MIMO $n_t \times n_r$ channel, $\forall\ n_r$.

Thus, in the following, we restrict our study to the case of symmetric channels $n_r = n_t$.

3.5 Non-Vanishing Determinant Codes

If a Space–Time code satisfies property (3.37), then it is approximately universal and if it is approximately universal, then it achieves the Diversity Multiplexing gain Trade-off of the MIMO channel. We derive here a simple sufficient condition for a Space–Time code to fulfill property (3.37). Consider a square $n_t \times n_t$ *linear dispersion* Space–Time block code [27]. The entries of a codeword $\mathbf{X}$ are thus linear combinations of information symbols. We suppose that these information symbols are carved from a QAM or an HEX constellation. Remark that both constellations are approximately universal for a SISO channel. Now suppose that there are, in the codeword $\mathbf{X}$, n_t^2 information symbols.

Finally, assume that we consider non-normalized information symbols, which means that, for example, (see Figure 3.3) the minimum distance of the constellation, d, remains the same when the spectral efficiency varies. It is obvious that if the minimum determinant of our code is lower bounded by some constant when the spectral efficiency increases, then this code fulfills condition (3.37). This leads to the definition of *non-vanishing determinant codes*.

Definition 3.7. A Space–Time block code $\mathcal{C}$ is a *non-vanishing determinant* code (NVD code) for an $n_t \times n_t$ MIMO channel if

(1) $\mathcal{C}$ is a linear dispersion code.
(2) Entries of the codewords depend on n_t^2 QAM or HEX information symbols.
(3) The minimum determinant of $\mathcal{C}$ is

$$\delta_{\min}(\mathcal{C}(R)) \triangleq \min_{\mathbf{X}\in\mathcal{C}\setminus\{0\}} |\det \mathbf{X}|^2 \geq \psi > 0, \tag{3.38}$$

where ψ does not depend on R, the spectral efficiency of the code.

A counterexample which is a vanishing determinant code can be found in [14]. This 2×2 STB code has a minimum determinant which tends to 0 when R increases.

NVD codes are a very important class of codes due to the following result (proved first in dimension 2 in [63] and then more generally in [20]):

Theorem 3.4. NVD codes are approximately universal codes and, thus, they achieve the DM trade-off.

Remark 3.1. The NVD property was introduced in Chapter 2 as a requirement to preserve the coding gain for the entire coding scheme. Here we have explained why the NVD property also implies achieving the DMT.

3.6 Information Preserving Codes

Trade-off achieving codes are optimal codes in the sense of the DMT. Among this family of codes, we will consider NVD codes which show a good behavior in the large SNR region and for large values of R. In order to design good codes for all regions of SNR, in Chapter 2 we discussed cubic shaping. Here we will find that cubic shaping results into another information theoretic property.

Definition 3.8. Assume a MIMO Gaussian channel with Gaussian inputs. A linear dispersion Space–Time code is *information lossless* if the mutual information of the equivalent channel obtained by including the encoder in the channel is equal to the mutual information of the MIMO channel. Note that, in Figure 3.4, this definition is equivalent to $I(X_1,Y_1) = I(X,Y)$.

The equivalent channel is obtained by vectorizing the received signal matrix. From

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \cdot \mathbf{X}_{n_t \times T} + \mathbf{Z}_{n_r \times T}, \tag{3.39}$$

where the subscripts indicate matrices dimensions and T is the temporal code length, we obtain the equivalent channel, given by

$$\begin{aligned} \mathrm{vec}(\mathbf{Y})_{n_r T \times 1} = & \begin{bmatrix} \mathbf{H} & & \\ & \ddots & \\ & & \mathbf{H} \end{bmatrix}_{n_r n_t \times n_r n_t} \\ & \times \mathbf{\Phi}_{n_r n_t \times n_t T} \cdot \begin{bmatrix} s_1 \\ \vdots \\ s_{n_t T} \end{bmatrix} + \mathrm{vec}(\mathbf{Z})_{n_r T \times 1}, \end{aligned} \tag{3.40}$$

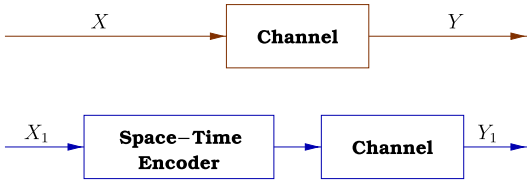

Fig. 3.4 Equivalent channel without and with the Space–Time encoder.

where s_i are the information symbols and $\mathbf{\Phi}$ is the matrix defining the linear dependencies between the entries of $\mathbf{X}$ and the information symbols.

Proposition 3.5. A linear dispersion Space–Time block code associated to a unitary matrix $\mathbf{\Phi}$ is an information lossless code.

Proof. The mutual information per channel use of the equivalent channel is

$$\begin{aligned} & I^{\mathrm{eq}}(\mathbf{X};\mathbf{Y}) \\ & \quad = \tfrac{1}{T}\log\det\left(\mathbf{I}_{n_r n_t} + \frac{\mathsf{SNR}}{n_t}\begin{bmatrix}\mathbf{H} & & \\ & \ddots & \\ & & \mathbf{H}\end{bmatrix}\mathbf{\Phi}\mathbf{\Phi}^{\dagger}\begin{bmatrix}\mathbf{H}^{\dagger} & & \\ & \ddots & \\ & & \mathbf{H}^{\dagger}\end{bmatrix}\right) \\ & \quad = \frac{1}{T}\log\det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^{\dagger}\right)^{T} \\ & \quad = \log\det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^{\dagger}\right) \end{aligned}$$

□

Remark 3.2. Note that once the matrix $\mathbf{\Phi}$ is chosen to be unitary, we automatically obtain the cubic shaping described in Section 2.5.

Chapters 2 and 3 have now settled the code design criteria to optimize in order to obtain efficient Space–Time codes. The next chapter will be dedicated to introducing the algebra background necessary to understand the construction of codes based on cyclic division algebras.

4

Cyclic Division Algebras

This chapter is devoted to the mathematical background necessary for building codes from cyclic division algebras. While introducing the definitions and results that we need, we keep in mind to emphasize the coding applications, alternating the theory with examples. The first section aims at introducing the notion of division algebra, the key concept for Space–Time coding, since it gives a way of building fully-diverse Space–Time codes. The Alamouti code is used as an illustration. In order to increase the throughput of the codes, we introduce algebras over number fields. Number fields will be shown to allow encoding of QAM and HEX constellations. Then a particular family of algebras, namely cyclic algebras built over number fields, will yield, for n transmit antennas, $n \times n$ Space–Time codewords that send n^2 information symbols encoded into n^2 signals. We further exploit the algebraic properties of a number field, and work in its ring of integers, which results, in terms of coding, in the non-vanishing determinant property. Finally, rings of integers of number fields can be used to build algebraic lattices. The lattice structure helps us to control the transmitted energy when encoding the Space–Time codes.

4.1 Fields and Algebras

The goal of this first section is to provide definitions and examples for algebraic structures such as *ring* and *field*, so as to end up with the notion of *algebra*. We end the section by describing the algebra of *Hamilton's quaternions*, which will be an example of *division algebra*.

4.1.1 Commutative and Non-Commutative Fields

Let $\mathbb{Z}$ be the set of rational integers $\{\ldots,-2,-1,0,1,2,\ldots\}$, $\mathbb{Q}$ be the set of rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \,|\, a,b \neq 0 \in \mathbb{Z}\right\}$, $\mathbb{R}$ denote the real numbers, and $\mathbb{C}$ the complex numbers.

Definition 4.1. Let A be a set endowed with two internal operations denoted by $+$ and $\cdot$

$$\begin{array}{ccc} A \times A & \to & A \\ (a,b) & \mapsto & a+b \end{array} \quad \text{and} \quad \begin{array}{ccc} A \times A & \to & A \\ (a,b) & \mapsto & a \cdot b \end{array}$$

The set $(A,+,\cdot)$ is a *ring* if

(1) $(A,+)$ is an Abelian (or commutative) group,
(2) the operation $\cdot$ is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in A$ and has a neutral element 1 such that $1 \cdot a = a \cdot 1$ for all $a \in A$,
(3) the operation $\cdot$ is distributive over $+$, i.e., $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a,b,c \in A$.

The ring A is *commutative* if $a \cdot b = b \cdot a$ for all $a,b \in A$. The set of elements of A that are invertible for the operation $\cdot$ is called the set of *units* of A, and is denoted by A^*.

The set $\mathbb{Z}$ is easily checked to be a ring. Its units are $\mathbb{Z}^* = \{1,-1\}$.

Definition 4.2. Let A be a ring such that $A^* = A \backslash \{0\}$. Then A is said to be a *skew field* or *division algebra*. If A is moreover commutative, it is said to be a *field*.

Looking the other way round, a division algebra is a non-commutative field. Division algebras will be our object of study for the rest of this chapter.

4.1.2 Algebras and Division Algebras

The most well known examples of fields are the sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. They are all commutative. In this section, we will present a non-commutative field, the *Hamilton's quaternions*, which will be used to build the Alamouti code.

Combining the more familiar notion of *vector space* with the one of ring, we arrive at the notion of *algebra*.

Definition 4.3. An algebra $\mathcal{A}$ is a set over a field K with operations of addition, multiplication, and multiplication by elements of K that have the following properties:

(1) $\mathcal{A}$ is a vector space with respect to addition and multiplication by elements of the field.
(2) $\mathcal{A}$ is a ring with respect to addition and multiplication.
(3) $(\lambda a)b = a(\lambda b) = \lambda(ab)$ for any $\lambda \in K$, a, $b \in \mathcal{A}$.

The set $\mathcal{M}_n(\mathbb{R})$ of $n \times n$ matrices with entries in $\mathbb{R}$ is an algebra over $\mathbb{R}$. It is a vector space of dimension n^2 over $\mathbb{R}$. It is a non-commutative ring with respect to the usual addition and multiplication of matrices.

The rest of this section is devoted to the most famous example of non-commutative field, the *Hamilton's quaternions*. It also has a structure of algebra, and will first be presented as such. Let $\{1, i, j, k\}$ be a basis for a vector space of dimension 4 over $\mathbb{R}$. These elements satisfy the rules $i^2 = -1$, $j^2 = -1$, $k^2 = -1$, and $k = ij = -ji$. The *Hamilton's quaternions* is the set $\mathbb{H}$ defined by

$$\mathbb{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}.$$

It has a structure of ring, since addition and multiplication are well-defined, though one has to be careful about the non-commutativity when doing computations! See Table 4.1 for the multiplication table.

Table 4.1 The multiplication table for the Hamilton's quaternions.

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Let us now prove that the Hamilton's quaternions are a division algebra, that is, every nonzero element $q \in \mathbb{H}$ is invertible. Like for complex numbers, one can define the *conjugate* of a quaternion $q = x + yi + zj + wk$ as

$$\bar{q} = x - yi - zj - wk.$$

It is a straightforward computation to check that

$$q\bar{q} = x^2 + y^2 + z^2 + w^2.$$

We call $\bar{q}q = q\bar{q} = |q|^2 = N(q)$ the *norm of a quaternion*. Since $x, y, z, w \in \mathbb{R}$, $q\bar{q} > 0$, unless $x = y = z = w = 0$. Thus the inverse of a quaternion q is given by

$$q^{-1} = \frac{\bar{q}}{q\bar{q}},$$

and all nonzero elements have an inverse.

We end this section by motivating why algebraic structures such as Hamilton's quaternions are of interest for coding purposes. Since coding for multiple antennas involves sending matrices, let us first see that there is a natural correspondence between elements of $\mathbb{H}$ and 2×2 matrices with coefficients in $\mathbb{C}$.

Note that any quaternion $q = x + yi + zj + wk$ can be written as

$$(x + yi) + (zj - wji) = \alpha_q + j\beta_q,$$

where $\alpha_q = x + yi \in \mathbb{C}$, $\beta_q = z - wi \in \mathbb{C}$. Thus $\mathbb{H}$ is a *right* $\mathbb{C}$-vector space (that is scalars multiply on the right), with $\mathbb{C}$-basis $\{1, j\}$. In this basis, $q = (\alpha_q, \beta_q)$. Note that $\mathbb{H}$ is *not* a $\mathbb{C}$-algebra. Consider the left multiplication by ν, that is $m_\nu(q) = \nu q$. In the basis $\{1, j\}$, we have

$$m_i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad m_j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad m_k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Check for example how k multiplies (on the left) the basis elements $\{1, j\}$

$$k(1,j) = (k, kj) = (ij, ijj) = (-ji, -i) = (1,j)\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

More generally, if $x, y \in \mathbb{R}$, we have

$$m_{x+yi} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} x+yi & 0 \\ 0 & \overline{x+yi} \end{pmatrix}.$$

Thus, for a general quaternion $\nu = \alpha_\nu + j\beta_\nu$ (α_ν, $\beta_\nu \in \mathbb{C}$) we have

$$m_\nu = \begin{pmatrix} \alpha_\nu & -\bar{\beta}_\nu \\ \beta_\nu & \bar{\alpha}_\nu \end{pmatrix}. \tag{4.1}$$

This construction gives a correspondence between an element ν in the Hamilton's quaternions and a 2×2 matrix with coefficients in $\mathbb{C}$ of the form (4.1).

Example 4.1 (The Alamouti code). Let $\mathcal{C}$ be the following set of matrices

$$\mathcal{C} = \left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}^T \mid \alpha,\ \beta \in \mathbb{C} \right\}.$$

It corresponds to the codewords of the Alamouti code, introduced in Section 3.4.3, where the code has been shown to be fully-diverse. The full-diversity can also be derived from the Hamilton's quaternions being a division algebra as follows.

Let $\nu = \alpha + j\beta \in \mathbb{H}$. If $\mathbf{X} = m_\nu \in \mathcal{C}$, then

$$\det(\mathbf{X}) = |\alpha|^2 + |\beta|^2 = N(\nu),$$

the norm of the quaternion ν. Thus $N(\nu) = 0 \iff \nu = 0$.

4.2 Algebras on Number Fields

In the previous section, we gave as example of algebra the Hamilton's quaternions, which are based on the field $\mathbb{R}$. In this section, we are interested in building algebras over *number fields*.

4.2.1 Introducing Number Fields

Consider the set of rational numbers $\mathbb{Q}$, which is easily checked to be a field. Other fields can be built starting from $\mathbb{Q}$. Take for example the element i, such that $i^2 = -1$, which is not an element of $\mathbb{Q}$. One can build a new field "adding" i to $\mathbb{Q}$, the same way i is added to $\mathbb{R}$ to create $\mathbb{C}$. Note that in order to make this new set a field, we have to add all the multiples and powers of i. We thus get a new field that contains both $\mathbb{Q}$ and i, and only $\mathbb{Q}$-linear combination of i, that we denote by $\mathbb{Q}(i)$. We call it a field extension of $\mathbb{Q}$. Note that we can iterate this procedure, and start with the field $\mathbb{Q}(i)$. Then, adding for example the element $\sqrt{5}$ (which does not belong to $\mathbb{Q}(i)$), its multiples and powers, we get a new field, denoted by $\mathbb{Q}(i, \sqrt{5})$. Thus $\mathbb{Q}(i, \sqrt{5})$ is an extension of $\mathbb{Q}(i)$, which is itself an extension of $\mathbb{Q}$. Let us formalize this procedure.

Definition 4.4. Let K and L be two fields. If $K \subseteq L$, we say that L is a *field extension* of K. We denote it by L/K.

It is useful to note that if L/K is a field extension, then L has a natural structure of vector space over K, where vector addition is addition in L and scalar multiplication of $a \in K$ on $v \in L$ is just $av \in L$. For example, an element $x \in \mathbb{Q}(i)$ can be written as $x = a + ib$, where $\{1, i\}$ are the basis "vectors" and $a, b \in \mathbb{Q}$ are the scalars. The dimension of $\mathbb{Q}(i)$ as vector space over $\mathbb{Q}$ is two. Similarly, an element of $\mathbb{Q}(i, \sqrt{5})$ can be written $w = x + y\sqrt{5}$, with $x, y \in \mathbb{Q}(i)$, or also $w = (a + ib) + \sqrt{5}(c + id)$, $a, b, c, d \in \mathbb{Q}$. Thus, $\mathbb{Q}(i, \sqrt{5})$ is a vector space of dimension two over $\mathbb{Q}(i)$, or of dimension four over $\mathbb{Q}$. It is often useful to draw a picture to see the hierarchy of fields (see Figure 4.1).

Definition 4.5. Let L/K be a field extension. The dimension of L as vector space over K is called the *degree* of L over K and is denoted by $[L : K]$. If $[L : K]$ is finite, we say that L is a *finite extension* of K.

A particular case of finite extension will be of great importance for our purpose.

$$\begin{array}{c} \mathbb{Q}(i,\sqrt{5}) \\ | \, 2 \\ \mathbb{Q}(i) \\ | \, 2 \\ \mathbb{Q} \end{array}$$

Fig. 4.1 This diagram shows field extensions, with the degree on the branches.

Definition 4.6. A finite field extension of $\mathbb{Q}$ is called a *number field*.

Remark 4.1. The number fields

$$\mathbb{Q}(i) = \{a + bi \mid a,b \in \mathbb{Q}\}, \quad \mathbb{Q}(j) = \{a + bj \mid a,b \in \mathbb{Q}\},$$

where j is a primitive 3rd root of unity ($j^3 = 1$ and $j^2 \neq 1$) are of particular interest. In fact, restricting a and b to $\mathbb{Z}$ we can obtain the set of *Gaussian integers* $\mathbb{Z}[i]$ and the set of *Eisenstein integers* $\mathbb{Z}[j]$ (see Definition 4.19). The QAM constellations are included in $\mathbb{Z}[i] + (1+i)/2$ while HEX constellations are included in $\mathbb{Z}[j]$.

Going on with our previous example, observe that a way to describe i is to say that this number is the solution of the equation $X^2 + 1 = 0$. Building $\mathbb{Q}(i)$, we thus add to $\mathbb{Q}$ the solution of a polynomial equation with coefficients in $\mathbb{Q}$, which is not in $\mathbb{Q}$.

Definition 4.7. Let L/K be a field extension, and let $\alpha \in L$. If there exists a nonzero irreducible monic (with highest coefficient 1) polynomial $p \in K[X]$ such that $p(\alpha) = 0$, we say that α is *algebraic* over K. Such a polynomial is called the *minimal polynomial* of α over K. We denote it by p_α.

In our example, the polynomial $X^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$. The number i is algebraic over $\mathbb{Q}$. Similarly, $X^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(i)$.

Definition 4.8. If all the elements of L are algebraic over K, we say that L is an *algebraic extension* of K.

Remark 4.2. Since it can be shown that a finite extension is an algebraic extension (see [54, p. 23]), we also call equivalently a number field (c.f. Definition 4.6) an *algebraic number field*.

4.2.2 Embeddings and Galois Group

Now that we set up the framework, we will concentrate on the particular family of fields that are number fields, that is field extensions $K/\mathbb{Q}$, with $[K:\mathbb{Q}]$ finite. In the following, K will denote a number field.

We start with a result which simplifies the way of describing a number field.

Theorem 4.1 [54, p. 40]. If K is a number field, then $K = \mathbb{Q}(\theta)$ for some algebraic number $\theta \in K$, called *primitive element*.

As a consequence of Theorem 4.1, K is a $\mathbb{Q}$-vector space generated by the powers of θ. If K has degree n over $\mathbb{Q}$, then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a *basis* of K, i.e., $x \in K$ can be written as $x = \sum_{i=0}^{n-1} x_i \theta^i$, $x_i \in \mathbb{Q}$, and the degree of the minimal polynomial of θ is n.

Example 4.2 (Primitive Element). Consider the number field $\mathbb{Q}(i, \sqrt{5})$. We will show that $\mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$. Clearly, $\mathbb{Q}(i + \sqrt{5}) \subseteq \mathbb{Q}(i, \sqrt{5})$. Now

$$(i + \sqrt{5})^3 = 14i + 2\sqrt{5} \in \mathbb{Q}(i + \sqrt{5}),$$

so that

$$(i + \sqrt{5})^3 - 2(i + \sqrt{5}) = 12i \in \mathbb{Q}(i + \sqrt{5}).$$

Thus i, and consequently $\sqrt{5}$ belong to $\mathbb{Q}(i + \sqrt{5})$. A basis of $\mathbb{Q}(i, \sqrt{5})$ over $\mathbb{Q}$ is for example given by $\{1, i + \sqrt{5}, (i + \sqrt{5})^2, (i + \sqrt{5})^3\}$.

We will now see how a number field K can be represented, we say *embedded*, into $\mathbb{C}$. Recall that if A and B are rings, a *ring homomorphism* is a map $\psi : A \to B$ that satisfies, for all $a, b \in A$

(1) $\psi(a + b) = \psi(a) + \psi(b)$
(2) $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$
(3) $\psi(1) = 1$

Definition 4.9. Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be two field extensions of $\mathbb{Q}$. We call $\varphi : K \to L$ a $\mathbb{Q}$-*homomorphism* if φ is a ring homomorphism that satisfies $\varphi(a) = a$ for all $a \in \mathbb{Q}$, i.e., that *fixes* $\mathbb{Q}$.

Definition 4.10. A $\mathbb{Q}$-homomorphism $\varphi : K \to \mathbb{C}$ is called an *embedding* of K into $\mathbb{C}$.

Note that an embedding is an injective map, so that we can really understand it as a way of representing elements of K as complex numbers.

Theorem 4.2. [54, p. 41] Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. There are exactly n distinct embeddings of K into $\mathbb{C}$: $\sigma_i : K \to \mathbb{C}$, $\sigma_i(\theta) = \theta_i$, $i = 1, \ldots, n$, where θ_i are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$.

Notice that one of the σ_i, say σ_1, is the identity mapping, i.e., $\sigma_1(x) = x$, for all $x \in K$. When we apply the embedding σ_i to an arbitrary element x of K, $x = \sum_{k=1}^{n} a_k \theta^k$, $a_k \in \mathbb{Q}$, we get, using the properties of $\mathbb{Q}$-homomorphisms

$$\begin{aligned} \sigma_i(x) &= \sigma_i\left(\sum_{k=1}^{n} a_k \theta^k\right),\ a_k \in \mathbb{Q} \\ &= \sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k \theta_i^k \in \mathbb{C} \end{aligned}$$

and we see how the image of any x under σ_i is uniquely identified by θ_i.

For example, since $X^2+1=(X+i)(X-i)$, there are two embeddings

$$\begin{aligned}\sigma_1: \quad & \mathbb{Q}(i)\to\mathbb{C}\\ & a+bi\mapsto a+bi\\ \sigma_2: \quad & \mathbb{Q}(i)\to\mathbb{C}\\ & a+bi\mapsto a-bi\end{aligned}$$

It is interesting to notice in this example that both embeddings are also mappings from $\mathbb{Q}(i)$ to itself. This is not always the case. Consider for example, the polynomial

$$X^3-2=(X-j\sqrt[3]{2})(X-j^2\sqrt[3]{2})(X-\sqrt[3]{2}),$$

where j is a primitive 3rd root of unity. Consider now the field $\mathbb{Q}(\sqrt[3]{2})$. We have the three embeddings

$$\begin{aligned}\sigma_1: \mathbb{Q}(\sqrt[3]{2})&\to\mathbb{C}\\ \sqrt[3]{2}&\mapsto\sqrt[3]{2}\\ \sigma_2: \mathbb{Q}(\sqrt[3]{2})&\to\mathbb{C}\\ \sqrt[3]{2}&\mapsto j\sqrt[3]{2}\\ \sigma_3: \mathbb{Q}(\sqrt[3]{2})&\to\mathbb{C}\\ \sqrt[3]{2}&\mapsto j^2\sqrt[3]{2}\end{aligned}$$

But since $\mathbb{Q}(\sqrt[3]{2})\neq\mathbb{Q}(j\sqrt[3]{2})$, σ_2 is not a mapping from $\mathbb{Q}(\sqrt[3]{2})$ to itself. In the following, we will need to restrict ourselves to number fields whose embeddings are mappings to themselves. Let us now formalize the concept.

When σ_i, $i=1,\ldots,n$ are defined from K to K, note that they are just a permutation of the roots of the minimal polynomial. They are then bijective (and thus called $\mathbb{Q}$-*automorphisms* of K, that is, maps from a field to itself that are bijective and fix $\mathbb{Q}$).

Such automorphisms do not only exist for an extension $K/\mathbb{Q}$. Consider again our example with $\mathbb{Q}(i,\sqrt{5})$, as a field extension of degree two of $\mathbb{Q}(i)$. It can be defined, as already pointed out, by the polynomial X^2-5 over $\mathbb{Q}(i)$. Since $X^2-5=(X-\sqrt{5})(X+\sqrt{5})$, both

$\pm\sqrt{5} \in \mathbb{Q}(i,\sqrt{5})$, we can define two automorphisms of $\mathbb{Q}(i,\sqrt{5})$ as follows, $a,b \in \mathbb{Q}(i)$:

$$\begin{aligned} \sigma_1 : \quad & \mathbb{Q}(i,\sqrt{5}) \to \mathbb{C} \\ & a + b\sqrt{5} \mapsto a + b\sqrt{5} \\ \sigma_2 : \quad & \mathbb{Q}(i,\sqrt{5}) \to \mathbb{C} \\ & a + b\sqrt{5} \mapsto a - b\sqrt{5} \end{aligned}$$

Notice that σ_1 and σ_2 are $\mathbb{Q}(i)$-automorphisms of $\mathbb{Q}(i,\sqrt{5})$, that is, they satisfy $\sigma_j(x) = x$, $j = 1,2$, for all $x \in \mathbb{Q}(i)$.

These examples about field automorphisms prepared us for the following theorem and definition:

Theorem 4.3 [54, p. 72]. Let L/K be a field extension. The set of K-automorphisms of L forms a group under composition of maps.

Though this result is not hard to prove, it is fundamental for a whole theory called *Galois Theory*. Let us give its first definitions.

Definition 4.11. A number field extension L/K is a *Galois extension* if every irreducible polynomial over K which has at least one zero in L has in fact all its zeroes in L. The *Galois group* of the extension L/K, denoted by $\mathrm{Gal}(L/K)$, is the group of all K-automorphisms of L under composition of maps.

We have already noticed that both embeddings of $\mathbb{Q}(i)$ are mappings from $\mathbb{Q}(i)$ to itself. In other words, both roots of the minimal polynomial $X^2 + 1$ belong to $\mathbb{Q}(i)$. Thus $\mathbb{Q}(i)/\mathbb{Q}$ is a Galois extension. The two embeddings σ_1, σ_2 of $\mathbb{Q}(i)$ form a group with two elements for the law given by the composition. The identity is given by σ_1, and since $\sigma_2(\sigma_2(x)) = x$ for all $x \in \mathbb{Q}(i)$, σ_2 is invertible. Thus $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{Id}, a + ib \mapsto a - ib\}$. Similarly $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)) = \{\mathrm{Id}, a + \sqrt{5}b \mapsto a - \sqrt{5}b\}$.

Notice that in both examples, the Galois group is generated by one element, that is, all the elements of the group are obtained as the powers of one element of the group. We call such a group a *cyclic group*.

Definition 4.12. A *cyclic group* G is a group generated by one element. Writing the group law multiplicatively, we have $G = \{g, g^2, \ldots, g^{n-1}, 1\}$ if G has n elements. We denote $G = \langle g \rangle$.

We will usually denote a cyclic Galois group by $\langle \sigma \rangle$, where σ is the generator of the group.

We close this section with the following remark. We have shown that the polynomial $X^3 - 2$ over $\mathbb{Q}$ yields three embeddings that are not automorphisms of $\mathbb{Q}(\sqrt[3]{2})$. One may also have considered adding the roots of $X^3 - 2$ to $\mathbb{Q}(i)$ instead of $\mathbb{Q}$. We then still have the three embeddings given by the three roots of $X^3 - 2$. To differentiate them, we call them *relative embeddings*.

Definition 4.13. Let L/K be a field extension of degree n. We call *relative embeddings* the n K-homomorphisms (i.e., homomorphisms fixing K) of L into $\mathbb{C}$.

4.2.3 Introducing Cyclic Algebras

We are now ready to define our main object of study, namely the family of cyclic algebras.

Definition 4.14. Let L/K be a Galois extension of degree n such that its Galois group $G = \mathrm{Gal}(L/K)$ is cyclic, with generator σ. Choose an element $0 \neq \gamma \in K$. We construct a non-commutative algebra, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus \cdots \oplus e^{n-1}L$$

such that e satisfies

$$e^n = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \qquad \text{for } \lambda \in L,$$

and $\oplus$ denotes the direct sum. Such an algebra is called a *cyclic algebra*.

We first comment this definition. The algebra $\mathcal{A}$ is defined as a direct sum of copies of L, which gives its vector space structure and means

that an element x in the algebra is written as

$$x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1},$$

with $x_i \in L$. To define its ring structure, we need a multiplication. Since the algebra is non-commutative, the rule $\lambda e = e\sigma(\lambda)$ explains how to do computations when the element e is multiplied on the left. By analogy, one may think of the rule $ij = -ji$ defined for the Hamilton's quaternions.

The reason why these cyclic algebras are interesting for our purpose is the existence of a correspondence[1] between an element x of the algebra $\mathcal{A}$ and a matrix $\mathbf{X} \in \mathcal{M}_n(L)$. Let $x \in \mathcal{A}$, and as for the Hamilton's quaternions, consider the left multiplication of an element of the algebra by x in the basis $\{1, e, e^2, \ldots, e^{n-1}\}$. The matrix of left multiplication by x can be checked to be given by

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \ldots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{4.2}$$

We illustrate the computation on an example. For $n = 2$, we have

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1 \\ &= (x_0y_0 + \gamma\sigma(x_1)y_1) + e(\sigma(x_0)y_1 + x_1y_0), \end{aligned}$$

since $e^2 = \gamma$. In matrix form, in the basis $\{1, e\}$, this yields

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}.$$

[1] To be rigorous, one can show that there is an isomorphism between the algebra $\mathcal{A} \otimes_K L$ and $\mathcal{M}_n(L)$.

Example 4.3 (Encoding codes from cyclic algebras). Similarly to the Alamouti code in Example 4.1, codebooks for two antennas made from cyclic algebras have the following form:

$$\mathcal{C} = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}^T | \, x_0,\ x_1 \in L \right\},$$

where we consider the cyclic extension L/K.

Let us now discuss the encoding and the rate of such codes. Suppose that the information symbols to be sent are carved from QAM or HEX constellations.

If x belongs to a cyclic algebra $\mathcal{A}$, then $x = \sum_{k=0}^{n-1} e^k x_k$. Recall that the coefficients x_i, $i = 0, \ldots, n-1$, are elements of a field L, which is an extension of K. Consider our example, where $L = \mathbb{Q}(i, \sqrt{5})$. Then

$$x_0 = a_0 + \sqrt{5}b_0, \quad x_1 = a_1 + \sqrt{5}b_1, \quad a_0, a_1, b_0, b_1 \in \mathbb{Q}(i).$$

Since QAM symbols can be seen as elements of $\mathbb{Q}(i)$ (from Remark 4.1), they belong to the base field $K = \mathbb{Q}(i)$. So both x_0 and x_1 encode two QAM information symbols, a_0, b_0 and a_1, b_1, respectively.

In general, if L/K has degree n, each coefficient x_k of $x = \sum_{k=0}^{n-1} e^k x_k$ will encode n information symbols. Since the element $x \in \mathcal{A}$ has n coefficients, it encodes n^2 information symbols. Codes made from cyclic algebras are said to be *full rate* (see Section 2.3), in the sense that they transmit n^2 signals that encode n^2 information symbols. In our previous example, the codebook is given by

$$\mathcal{C} = \left\{ \begin{pmatrix} a_0 + \sqrt{5}b_0 & \gamma(a_1 - \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & a_0 - \sqrt{5}b_0 \end{pmatrix}^T | \, a_0, a_1, b_0, b_1 \in Q\text{-QAM} \right\}.$$

where γ will be chosen in order to optimize the code performance as we will see in the following.

Remark 4.3. Since commonly used signal constellations are QAM and HEX, this means that we consider field extensions L/K where

K is either $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$, where j is a primitive 3rd root of unity, by Remark 4.1.

Note that the same n information symbols are distributed within one *layer* of the codeword.

Definition 4.15. We define a layer (or thread [18]) ℓ, for $\ell = 1, \ldots, n$, of the codeword the set of matrix entries in positions

$$(k, (\ell + k - 1) \bmod(n) + 1), \text{ for } k = 1, \ldots, n.$$

4.3 Norm and Ring of Integers

In the previous section, we introduced cyclic algebras, and showed how to build them. We are now interested in their properties, and how to use them to get good Space–Time codes. In particular, we will explain how to get full diversity, and furthermore *non-vanishing determinants*.

4.3.1 Norm and Full-Diversity

With the notion of embeddings (see Definition 4.13), we first define two quantities that will appear to be very useful, namely the *norm* and the *trace* of an algebraic element.

Definition 4.16. Let L/K be a field extension of degree n, where $\sigma_1, \ldots, \sigma_n$ denote the n relative embeddings of L. Let $x \in L$. The elements $\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)$ are called the *conjugates* of x and

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), \quad \mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

are called, respectively, the *norm* and the *trace* of x.

Whenever the context is not clear, we write $\mathrm{Tr}_{L/K}$, resp. $N_{L/K}$ to avoid ambiguity.

A definition of norm is also available for an element of a cyclic algebra.

Definition 4.17. Let x be an element of a cyclic algebra $\mathcal{A}$. Then the determinant of its corresponding matrix, as given in (4.2), is called the *reduced norm* of x.

In order to determine whether a code $\mathcal{C}$ is fully diverse, recall from Section 2.2 that we have to check that $\det(\mathbf{X}_i - \mathbf{X}_j) \neq 0$, for any $\mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}$. By linearity of the algebra, codes from cyclic algebras satisfy

$$\det(\mathbf{X}_i - \mathbf{X}_j) = \det(\mathbf{X}), \quad \mathbf{X}_i \neq \mathbf{X}_j, \quad \mathbf{X} \in \mathcal{C}.$$

We are thus interested in knowing when $\det(\mathbf{X}) \neq 0$ for all $\mathbf{X} \neq \mathbf{0}$, or equivalently, when $\mathcal{A}$ is a division algebra (i.e., all elements of $\mathcal{A}$ are invertible, see Definition 4.2).

Definition 4.18. A cyclic algebra which is also a division algebra is called a *cyclic division algebra*.

Let us now determine when a cyclic algebra is actually a cyclic division algebra.

Example 4.4 (An algebra of degree 2). If $n = 2$, we have

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0) - \gamma x_1 \sigma(x_1) = N_{L/K}(x_0) - \gamma N_{L/K}(x_1).$$

Thus

$$\det(\mathbf{X}) = 0 \iff \gamma = N_{L/K}\left(\frac{x_0}{x_1}\right),$$

since multiplicativity of the norm follows from the multiplicativity of the relative embeddings. We thus have to check whether γ is a norm of some element of L.

A statement similar to the above one for determining whether a cyclic algebra is a division algebra is in fact true for any dimension n, though it cannot be proved the same way.

Proposition 4.4 [45, p. 279]. Let L/K be a cyclic extension of degree n with Galois group $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. If $0 \neq \gamma, \gamma^2, \ldots, \gamma^{n-1} \in K$ are not a norm of some element of L, then $(L/K, \sigma, \gamma)$ is a cyclic division algebra.

4.3.2 Ring of Integers and Non-Vanishing Determinants

In this section, we are interested in showing something beyond the full-diversity, namely, giving a lower bound on the determinant of the difference of two matrices. This property is called *non-vanishing determinant*. We let the reader refer to Sections 2.5 and 3.5 to recall why such a property is useful. In order to reach our goal, we need to introduce a new concept, *the ring of integers* of a number field K.

One of the first goals of algebraic number theory was to study the solutions of polynomial equations with coefficients in $\mathbb{Z}$. Given the equation

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0, \quad a_i \in \mathbb{Z} \quad \text{for all } i,$$

what can we say about its solutions? It is first clear that there may be solutions not in $\mathbb{Q}$, as $\sqrt{5}$ or i, which means that in order to find the solutions, we have to consider fields larger than $\mathbb{Q}$.

Definition 4.19. We say that $\alpha \in K$ is an *algebraic integer* if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of K is a ring called the *ring of integers* of K, denoted by $\mathcal{O}_K$.

The fact that the algebraic integers of K form a ring is a strong result [54, p. 47], which is not so easy to see. The natural idea that comes to mind is to find the corresponding minimal polynomial. Take $\sqrt{2}$ and 2. Both are algebraic integers of $\mathbb{Q}(\sqrt{2})$. How easy is it to find the minimal polynomial of $\sqrt{2} + 2$? How easy is it to find such a polynomial in general?

In this example, it can be shown [54, p. 60] that the algebraic integers are the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$. Similarly, the ring of integers of $\mathbb{Q}(i)$ is given by $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$. Care should be taken

in generalizing this result (see the following example). Note that $\mathbb{Z}[\sqrt{2}]$ is a ring since it is closed under all operations except for the inversion. For example $(2+2\sqrt{2})^{-1} = (2-\sqrt{2})/6$ does not belong to $\mathbb{Z}[\sqrt{2}]$.

In the following, we will first look at the structure of $\mathcal{O}_K$, the ring of integers of a number field. In the special case $K = \mathbb{Q}(i)$, we have seen that $\mathcal{O}_K = \mathbb{Z}[i]$, which means that $\mathcal{O}_K$ has a basis over $\mathbb{Z}$ given by $\{1, i\}$. We call $\mathcal{O}_K$ a $\mathbb{Z}$-*module*. An A-module, where A is a ring, is a generalization of the notion of K-vector space, where K is a field. In our case, we have that K has a structure of vector space over the field $\mathbb{Q}$, while we only have a structure of module for $\mathcal{O}_K$ over the ring $\mathbb{Z}$. This is formalized as follows:

Theorem 4.5 [54, p. 51]. Let K be a number field of degree n. The ring of integers $\mathcal{O}_K$ of K forms a free $\mathbb{Z}$–module of rank n (that is, there exists a basis of n elements over $\mathbb{Z}$).

Definition 4.20. Let $\{\omega_i\}_{i=1}^n$ be a basis of the $\mathbb{Z}$–module $\mathcal{O}_K$, so that we can uniquely write any element of $\mathcal{O}_K$ as $\sum_{i=1}^n a_i\omega_i$ with $a_i \in \mathbb{Z}$ for all i. We say that $\{\omega_i\}_{i=1}^n$ is an *integral basis* of K.

We give another example of number field, where we summarize the different notions seen so far.

Example 4.5 (Ring of Integers and Basis). Take $K = \mathbb{Q}(\sqrt{5})$. We know that any algebraic integer β in K has the form $a + b\sqrt{5}$ with some $a, b \in \mathbb{Q}$, such that the polynomial $p_\beta(X) = X^2 - 2aX + a^2 - 5b^2$ has integer coefficients. By simple arguments it can be shown that all the elements of $\mathcal{O}_K$ take the form $\beta = (u + v\sqrt{5})/2$ with both u, v integers with the same parity. So we can write $\beta = h + k(1+\sqrt{5})/2$ with $h, k \in \mathbb{Z}$. This shows that $\{1, (1+\sqrt{5})/2\}$ is an integral basis. The basis $\{1, \sqrt{5}\}$ is not integral since $a + b\sqrt{5}$ with $a, b \in \mathbb{Z}$ is only a subset of $\mathcal{O}_K$. Note that, $(1+\sqrt{5})/2$ is also a primitive element of K with minimal polynomial $X^2 - X - 1$.

Consider again the example $L = \mathbb{Q}(i, \sqrt{5})$. In Definition 4.19, its ring of integers $\mathcal{O}_L$ has been described as having a $\mathbb{Z}$-basis. Since $\mathbb{Q}(i, \sqrt{5})$ is an extension of degree 2 of $\mathbb{Q}(i)$, one may wonder about the existence of a $\mathbb{Z}[i]$-basis for $\mathcal{O}_L$. It does indeed exist, and it can be shown that

$$\mathcal{O}_L = \mathbb{Z}[i][(1+\sqrt{5})/2] = \left\{ u + v\frac{1+\sqrt{5}}{2} \mid u, v \in \mathbb{Q}(i) \right\}.$$

Thus $\{1, (1+\sqrt{5})/2\}$ is a $\mathbb{Z}[i]$-basis for $\mathcal{O}_L$. Note that in that sense, $(1+\sqrt{5})/2$ is an algebraic integer since it has a minimal polynomial $X^2 - X - 1 \in \mathbb{Z}[i][X]$.

Theorem 4.6 [54, p. 54]. Let L/K be a field extension. For any $x \in L$, we have $N_{L/K}(x)$ and $\mathrm{Tr}_{L/K}(x) \in K$. If $x \in \mathcal{O}_L$, we have $N_{L/K}(x)$ and $\mathrm{Tr}_{L/K}(x) \in \mathcal{O}_K$.

Let us illustrate this last result. The roots of the minimal polynomial $X^2 - X - 1$ are $\theta = (1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$. Thus

$$\sigma_1(\theta) = (1+\sqrt{5})/2 \quad \text{and} \quad \sigma_2(\theta) = (1-\sqrt{5})/2.$$

We have

$$\begin{aligned} X^2 - X - 1 &= (X - \sigma_1(\theta))(X - \sigma_2(\theta)) \\ &= X^2 - X(\sigma_1(\theta) + \sigma_2(\theta)) + \sigma_1(\theta)\sigma_2(\theta) \\ &= X^2 - \mathrm{Tr}(\theta)X + N(\theta). \end{aligned}$$

Since $\mathrm{Tr}_{\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)}(\theta) = \mathrm{Tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\theta) = 1$ and $N_{\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)}(\theta) = N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\theta) = -1$, they are indeed in $\mathbb{Z}$, the ring of integers of $\mathbb{Q}$, and thus in $\mathbb{Z}[i]$, the ring of integers of $\mathbb{Q}(i)$. Note that by definition, an element of $\mathcal{O}_L$ is root of a polynomial whose coefficients are in $\mathbb{Z}$.

Let us now come back to the computation of the minimum determinant. Consider the case $n = 2$. We have seen in Example 4.4 that

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = N_{L/K}(x_0) - \gamma N_{L/K}(x_1).$$

We now show how to get the *non-vanishing determinant* property in two steps:

(1) First, since $x_0, x_1 \in L$, by Theorem 4.6, $N_{L/K}(x_0)$ and $N_{L/K}(x_1)$ are in K. Since $\gamma \in K \subset L$, then $\det(\mathbf{X}) \in K$.
(2) Now, if we restrict $x_0, x_1 \in \mathcal{O}_L$, then again by Theorem 4.6, we get that $N_{L/K}(x_0)$ and $N_{L/K}(x_1)$ are in $\mathcal{O}_K$. By choosing $\gamma \in \mathcal{O}_K$, we conclude that $\det(\mathbf{X}) \in \mathcal{O}_K$.

When transmitting QAM or HEX symbols, we noticed in Remark 4.3 that K has to be $\mathbb{Q}(i)$, resp. $\mathbb{Q}(j)$. Since $\mathbb{Z}[i]$, resp. $\mathbb{Z}[j]$ is included in $\mathcal{O}_L$, by taking a suitable $\gamma \in \mathcal{O}_K$, we have that

$$\det(\mathbf{X}) \in \mathbb{Z}[i], \mathbb{Z}[j] \Rightarrow |\det(\mathbf{X})|^2 \in \mathbb{Z}$$

so that

$$|\det(\mathbf{X})|^2 \geq 1, \quad \mathbf{X} \neq \mathbf{0}.$$

In other words, this means that prior to SNR normalization, the minimum determinant does not depend on the spectral efficiency, which motivated the term "non-vanishing determinant".

This procedure can be generalized to higher dimensions n. However, the first step cannot be proved the same way, since explicit computations of the determinant in higher dimension gets more complicated. We need

---

Theorem 4.7 [49, p. 296 and p. 316]. Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic algebra, then its reduced norm belongs to K.

Then similarly, the coefficients $x_0, \ldots, x_{n-1}$ are chosen in $\mathcal{O}_L$, and γ has to be chosen in $\mathcal{O}_K$.

Remark 4.4 Note that forcing γ to be in $\mathcal{O}_K$ is a strong requirement. It may not always be possible to find such a γ. In [21], the authors show how the *non-vanishing determinant* property can be further obtained in considering $\gamma \in K$. The idea is that if $\gamma \in K$, then $\gamma = \gamma_n/\gamma_d$, with $\gamma_n, \gamma_d \in \mathcal{O}_K$. By putting into factor the denominator, one can use again the above argument. An example of this procedure will be detailed in the next chapter, Section 5.5.

4.4 Shaping, Lattices and Discriminant

To briefly summarize, we have seen so far how cyclic division algebras of degree n over L/K yield $n \times n$ linear Space–Time block codes, encoding n^2 information symbols, with full diversity. Furthermore, if the coefficients of the Space–Time code are chosen in the ring of integers $\mathcal{O}_L$, and with the parameter $\gamma \in \mathcal{O}_K$, we obtain the non-vanishing property, that is, a lower bound on the minimum determinant that does not depend, prior to SNR normalization, on spectral efficiency.

In this section, we first show how the structure of the ring of integers can be further exploited to construct an *algebraic lattice*. We then show how algebraic lattices can be useful to define a *shaping* property (see Section 2.5) on the constellation to be sent.

4.4.1 Algebraic Lattices

Let us give here the minimum necessary background on algebraic lattices. The interested reader can refer to [3, 4]. A self contained introduction to algebraic lattices can also be found in [43].

Algebraic lattices are built using the so-called canonical embedding of a number field:

Definition 4.21 Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of a number field K, and let us order the σ_is so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. Note that $r_1 + 2r_2 = n$. We call *canonical embedding* $\sigma : K \to \mathbb{R}^{r_1+2r_2}$ the isomorphism defined by

$$\begin{aligned}\sigma(x) = (&\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \\ &\Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)).\end{aligned}$$

We can define a similar embedding if we consider instead of the extension $K/\mathbb{Q}$ a more general extension L/K:

$$\begin{aligned}\sigma : \quad & L \to \mathbb{C}^n \\ & x \mapsto \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)),\end{aligned}$$

where $\sigma_1,\ldots,\sigma_n$ are relative embeddings of L/K, i.e., σ_i fixes K for all i.

Recall [11, 43] that a lattice Λ can be expressed by means of its generator matrix M

$$\Lambda = \{\mathbf{x} = \boldsymbol{\lambda} M \ \in \mathbb{R}^n \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}.$$

The lattice generator matrix M of an algebraic lattice, that is, of a lattice built using the canonical embedding of K, is given by

$$\begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1),\ldots,\Im\sigma_{r_1+r_2}(\omega_1) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n),\ldots,\Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix},$$

where $\{\omega_1,\ldots,\omega_n\}$ is here a basis of $\mathcal{O}_K$. This gives a real lattice.

Similarly, a complex lattice Λ^c is given by

$$\Lambda^c = \{\mathbf{x} = \boldsymbol{\lambda} M \ \in \mathbb{C}^n \mid \boldsymbol{\lambda} \in \mathbb{Z}[i]^n \text{ or } \mathbb{Z}[j]^n\}.$$

Now its generator matrix is given, using the embedding $\sigma(x) = (\sigma_1(x),\ldots,\sigma_n(x))$, by

$$\begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \ldots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix}, \tag{4.3}$$

where $\{\omega_1,\ldots,\omega_n\}$ is a basis of $\mathcal{O}_L$ over K, and $\sigma_1,\ldots,\sigma_n$ are relative embeddings of L/K.

Example 4.6 (Algebraic Lattices). Figure 4.2 shows an algebraic lattice from $K = \mathbb{Q}(\sqrt{5})$. As seen before (see Example 4.5), the integral basis of K is $\{1, \frac{1+\sqrt{5}}{2}\}$. The two embeddings are $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$ and the lattice generator matrix becomes

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}.$$

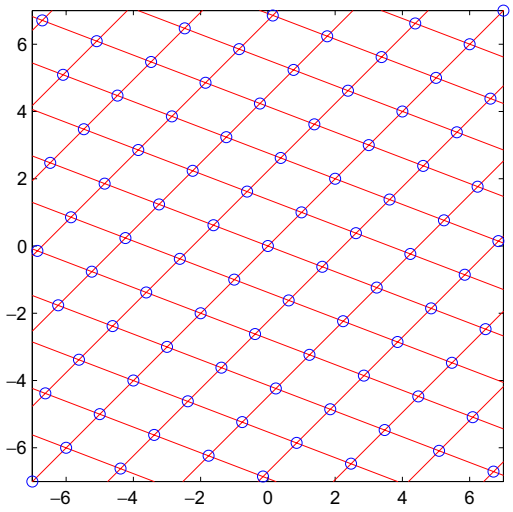

Fig. 4.2 Algebraic lattices from $\mathbb{Q}(\sqrt{5})$.

So far, we have used the ring of integers $\mathcal{O}_L$ to build algebraic lattices. In the following, we will show how algebraic lattices can be obtained in a more general manner, by considering *ideals* of $\mathcal{O}_L$.

Definition 4.22 An *ideal* $\mathcal{I}$ of a commutative ring A is an additive subgroup of A which is stable under multiplication by A, i.e., $a\mathcal{I} \subseteq \mathcal{I}$ for all $a \in A$.

Among all the ideals of a ring, some of them have the special property of being generated by only one element. These will be of particular interest for us.

Definition 4.23 An ideal $\mathcal{I}$ is *principal* if it is of the form:

$$\mathcal{I} = (x)A = \{xy,\ y \in A\}, \quad x \in \mathcal{I}.$$

If A is clear from the context, we may write $\mathcal{I} = (x)$.

Example 4.7 (Principal Ideals). If $R = \mathbb{Z}$, we have that $n\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$ for all n.

We can define the *norm* of an ideal. In the case of a principal ideal, it is directly related to the norm of a generator of the ideal.

Definition 4.24 Let $\mathcal{I} = (x)\mathcal{O}_L$ be a principal ideal of $\mathcal{O}_L$. Its *norm* is defined by $N(\mathcal{I}) = |N(x)|$.

An algebraic lattice Λ' built from an ideal $\mathcal{I} \subset \mathcal{O}_L$ gives a sublattice [11, 43] of the algebraic lattice Λ built from $\mathcal{O}_L$. If $\mathcal{I} = \alpha\mathcal{O}_L$, then the generator matrix M is given by

$$M = \begin{pmatrix} \sigma_1(\alpha\omega_1) & \sigma_2(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_1) \\ \sigma_1(\alpha\omega_2) & \sigma_2(\alpha\omega_2) & \dots & \sigma_n(\alpha\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\alpha\omega_n) & \sigma_2(\alpha\omega_n) & \dots & \sigma_n(\alpha\omega_n) \end{pmatrix}, \tag{4.4}$$

where $\{\omega_1, \dots, \omega_n\}$ is a basis of $\mathcal{O}_L$ over K, and $\sigma_1, \dots, \sigma_n$ are the relative embeddings. Equivalently, the matrix (4.4) is the matrix (4.3) multiplied by the diagonal matrix

$$\begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix}.$$

Given the above lattice generator matrix, it is easy to compute the *determinant* of the lattice. By definition, we have

$$\det(\Lambda) = |\det(M)|^2 = |\det[\sigma_j(\alpha\omega_i)]|^2 = |N(\alpha)|^2 |\det[\sigma_j(\omega_i)]|^2.$$

This determinant is actually related to an *invariant* of the number field, called the *discriminant*. Let us first define the discriminant for an extension $K/\mathbb{Q}$.

Definition 4.25 Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be an integral basis of K. The *discriminant* of K is defined as $d_K = \det[\sigma_j(\omega_i)]^2$.(It can be shown that the discriminant is independent of the choice of a basis [48].)

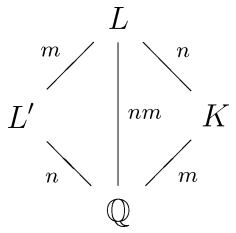

Fig. 4.3 The structure of the compositum field of of L' and K.

For code constructions given in Chapter 5, we will restrict ourselves to extension fields L/K of a special kind, namely $L/K = L'K/K$, i.e., L is the smallest field containing both L' and K. We call L the *compositum* of L' and K (see Figure 4.3). Furthermore, $L'K/K$ will have the property that the relative embeddings $\sigma_1,\ldots,\sigma_n$ of $L'K/K$ are actually the same as the embeddings of $L'/\mathbb{Q}$. This is certainly not true in general. Under this assumption we have that the determinant of the lattice is

$$\det(\Lambda) = |N_{K/\mathbb{Q}}(\alpha)|^2 |d_K|,$$

for a lattice built on $K/\mathbb{Q}$, while

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{L'}| \tag{4.5}$$

for a lattice built on the compositum $L'K/K$.

Example 4.8 (Discriminant). Let us compute the discriminant d_K of the field $\mathbb{Q}(\sqrt{5})$. Applying the two $\mathbb{Q}$-homomorphisms to the integral basis $\{\omega_1,\omega_2\} = \{1,(1+\sqrt{5})/2\}$, we obtain

$$d_K = \det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}^2 = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5.$$

The determinant of the lattice is 5.

4.4.2 Shaping

Let us now explain what we mean by a shaping constraint on the constellation to be sent in the case of cyclic algebra based codes.

In Section 2.5, the importance of constellation shaping in MIMO systems was explained on a small example. In Section 3.6, shaping was shown to be related to the information lossless property. It was proved that linear codes associated to a unitary matrix are information lossless. In the following, we will show how to obtain such a unitary matrix for cyclic algebra based codes.

Recall that a codeword (4.2) has the form:

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix},$$

where each layer (see Definition 4.15) is, up to multiplication by γ, of the form $(x_l, \sigma(x_l), \dots, \sigma^{n-1}(x_l))$, $l = 0, \dots, n-1$.

The shaping constraint requires that each layer of the codeword is of the form $M\mathbf{v}$, where M is a unitary matrix and $\mathbf{v}$ is a vector containing the information symbols. Let $\{\omega_1, \dots, \omega_{n-1}\}$ be a basis of $\mathcal{O}_L$. Each layer of a codeword is of the form:

$$\begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_n \\ \sigma(\omega_1) & \sigma(\omega_2) & \dots & \sigma(\omega_n) \\ & & & \\ \sigma^{n-1}(\omega_1) & \sigma^{n-1}(\omega_2) & \dots & \sigma^{n-1}(\omega_n) \end{pmatrix} \begin{pmatrix} u_{l,0} \\ u_{l,1} \\ \vdots \\ u_{l,n-1} \end{pmatrix} = \begin{pmatrix} x_l \\ \sigma(x_l) \\ \vdots \\ \sigma^{n-1}(x_l) \end{pmatrix} \tag{4.6}$$

for $x_l = \sum_{k=0}^{n-1} u_{l,k}\omega_{k+1} \in \mathcal{O}_L$. Since $u_{l,k}$ takes discrete values, we can see the above matrix multiplication as generating points in a lattice. The matrix M is thus the *generator matrix* of the lattice, whose *Gram matrix* is given by $MM^\dagger$.

We would like M to be unitary, which translates into saying that the lattice we would like to obtain for each layer is a $\mathbb{Z}[i]^n$–lattice, resp. a $\mathbb{Z}[j]^n$–lattice, since QAM and HEX symbols are finite subsets of $\mathbb{Z}[i]$, resp. $\mathbb{Z}[j]$. Note that the matrix M may be viewed as a precoding matrix applied to the information symbols.

Finally, note that the $2n^2$-dimensional real lattice generated by the vectorized codewords, where real and imaginary components are separated, is either $\mathbb{Z}^{2n^2}$ (for QAM constellation) or $A_2^{n^2}$ (for HEX constellation), where A_2 is the hexagonal lattice [11], with generator matrix

$$\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

Interpreting the unitary matrix M as the generator matrix of a lattice allows us to use the well studied theory of algebraic lattices briefly outlined above.

We have seen in (4.5) that the determinant of an algebraic lattice Λ built over a principal ideal $\mathcal{I} = (\alpha)\mathcal{O}_L$, where $L/K = L'K/K$, is given by

$$\det(\Lambda) = |N(\alpha)|^2 |d_{L'}|.$$

In order to get $\Lambda = \mathbb{Z}[i]^n$ (resp. $\mathbb{Z}[j]^n$), or a scaled version $\Lambda' = (c\mathbb{Z}[i])^n$ (resp. $(c\mathbb{Z}[j])^n$), a necessary condition is to find in $\mathcal{O}_L$ an element α of suitable norm, since

$$\det\left((c\mathbb{Z}[i])^n\right) = c^n.$$

Given an extension $L'K/K$, the discriminant is given. Thus one has to find an element α such that

$$|N(\alpha)|^2 |d_{L'}| = c^n.$$

This condition is however not sufficient, and once this element is found, one way to check that we indeed found the right lattice is to compute the Gram matrix $MM^\dagger$, and make sure we get the identity matrix. Since M is given by

$$\begin{pmatrix} \sigma_1(\alpha\omega_1) & \sigma_2(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_1) \\ \sigma_1(\alpha\omega_2) & \sigma_2(\alpha\omega_2) & \dots & \sigma_n(\alpha\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\alpha\omega_n) & \sigma_2(\alpha\omega_n) & \dots & \sigma_n(\alpha\omega_n) \end{pmatrix},$$

the Gram matrix can be computed as $MM^\dagger = [\mathrm{Tr}_{L/K}(\alpha\omega_i\overline{\omega_j})]$, where $\mathrm{Tr}_{L/K}$ is the trace of an element of $\mathcal{O}_L$. These two steps:

(1) finding an element α with the right norm in $\mathcal{O}_L$,
(2) computing the trace matrix $MM^\dagger$,

form the method we will use to obtain the shaping property on the constellation. The procedure will be illustrated for small numbers of antennas in the next chapter.

5

Perfect Space–Time Block Codes

This chapter is devoted to the definition and construction of *perfect Space–Time block codes*. We will now assemble the three preceding chapters, using the algebraic techniques presented in Chapter 4, to build Space–Time block codes (STBC) satisfying the design criteria explained in Chapters 2 and 3. We illustrate the code constructions for small numbers of antennas, namely up to six antennas. These constructions have been originally presented in [21, 44].

5.1 Definition of Perfect Space–Time Codes

Let us start by recalling what are the targeted code features. The two main design parameters for coherent Space–Time codes are:

- **Full diversity.** The rank criterion tells for square STBCs that full diversity is obtained if the determinant of the difference of two distinct codewords is nonzero:

$$\det(\mathbf{X}_i - \mathbf{X}_j) \neq 0, \quad \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}.$$

- **Minimum determinant.** The coding gain is given by the minimum determinant

$$\min_{\mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}} |\det(\mathbf{X}_i - \mathbf{X}_j)|^2.$$

In order to further improve the performance of Space–Time codes, we ask for two more properties, motivated in Chapters 2 and 3.

- **Non-vanishing determinant.** We say that a code has a *non-vanishing determinant* if, prior to SNR normalization, there is a lower bound on the minimum determinant that does not depend on the constellation size.
- **Shaping.** In order to optimize the energy efficiency of the codes, a shaping constraint on the signal constellation is introduced. The Q-QAM or Q-HEX to be sent are normalized according to the power at the transmitter. However, since we use linear STBCs, what is transmitted on each layer (see Definition 4.15) is a linear combination of information symbols, which may change the energy of the signal. Each layer can be written as $M\mathbf{v}$, where $\mathbf{v}$ is the vector containing the QAM or HEX information symbols, while M is a matrix that encodes the symbols into each layer. In order to get energy efficient codes, we ask the matrix M to be unitary. We will refer to this type of constellation shaping as *cubic shaping*, since a unitary matrix applied on a vector containing discrete values can be interpreted as generating points in a lattice. For example, if we use QAM symbols, we get the $\mathbb{Z}^n$ (cubic) lattice.

There is another property on which we do insist though it has not been stated yet, since it follows from the shaping constraint. However, let us make it explicit here.

- **Uniform average energy transmitted per antenna.** The ith antenna of the system will transmit a signal x_{ij} at time j. We ask that on average, the energy of each codeword entry is constant, in order to have a balanced repartition of the energy at the transmitter.

Having motivated the properties that an STBC should have to maximize its performance, we are now able to give the definition of a *perfect* Space–Time block code.

Definition 5.1 A square $n_t \times n_t$ STBC is called a *perfect* code if and only if:

- It is a full rate linear code using n_t^2 information symbols either QAM or HEX.
- The minimum determinant of the infinite code is nonzero (so that in particular the rank criterion is satisfied).
- The energy required to send the linear combination of the information symbols on each layer is similar to the energy used for sending the symbols themselves (we do not increase the transmitted energy in encoding the information symbols).
- It induces uniform average transmitted energy per antenna in all T time slots, i.e., all the coded symbols in the code matrix have the same average energy.

In the rest of this chapter, we will give the construction of perfect codes for $2, \ldots, 6$ antennas.

Remark 5.1 In Chapter 4, we have introduced as many algebraic techniques needed as possible, starting from no algebra background. This allows to explain almost all that is required to build the Space–Time codes, apart the non-norm element γ, the element such that none of its powers are a norm, needed to construct a division cyclic algebra. The techniques involved are far beyond the scope of this tutorial. For the sake of completeness, Subsection 5.2.1 gives one example of such techniques, in the simplest case, when the algebra is of degree 2. For more general dimensions, the interested reader may refer for example to [44] if γ is a root of unity, or more generally to [20, 36], and it has been shown in [21] that dividing a non-norm element by its conjugate still gives a non-norm element.

5.2 The Golden Code

The Golden code is a 2×2 perfect code. It has been found independently in [7, 15]. Its name, Golden code, comes from its algebraic construction [7], which involves the Golden number $\frac{1+\sqrt{5}}{2}$.

The Golden code is built using the cyclic algebra

$$\mathcal{A} = (L = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i),$$

with $\sigma : \sqrt{5} \mapsto -\sqrt{5}$. We have that

$$\mathcal{O}_L = \{a + b\theta \mid a, b \in \mathbb{Q}(i)\},$$

where $\theta = \frac{1+\sqrt{5}}{2}$. Before shaping, a codeword from this algebra is of the form:

$$\begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\sigma(\theta)) & a + b\sigma(\theta) \end{bmatrix},$$

with $a, b, c, d \in \mathbb{Z}[i]$. By definition, the codebook obtained is linear and full rate (since it contains the four information symbols a, b, c, d). It is also fully diverse since i is not a norm (see next subsection for a proof), and thus, $\mathcal{A}$ is a cyclic division algebra.

5.2.1 The Element $\gamma = i$ is Not a Norm in $\mathbb{Q}(i, \sqrt{5})$

We show here that the cyclic algebra $\mathcal{A}$ defining the Golden code is a division algebra [7]. The proof is given for sake of completeness, but uses some tools that are beyond the scope of this work.

Proposition 5.1 Let $K = \mathbb{Q}(i, \sqrt{5})$, then the element $\gamma = i$ is not a relative norm of any $x \in K$, i.e., $N_{K/\mathbb{Q}(i)}(x) \neq i, \forall x \in K$.

Proof. Let $\mathbf{Q}_5$ denote the field of 5-adic numbers, and $\mathbf{Z}_5 = \{x \in \mathbf{Q}_5 \mid \nu_5(x) \geq 0\}$ its valuation ring. The complex rationals $\mathbb{Q}(i)$ can be embedded in $\mathbf{Q}_5$ by

$$i \mapsto 2 + 5\mathbf{Z}_5.$$

Let $x = a + b\sqrt{5} \in K$ with $a, b \in \mathbb{Q}(i)$, then we must show that

$$N_{K/\mathbb{Q}(i)}(x) = a^2 - 5b^2 = i$$

has no solution for $a, b \in \mathbb{Q}(i)$. We can lift this equation in the 5-adic field $\mathbf{Q}_5$

$$a^2 - 5b^2 = 2 + 5x \ a, b \in \mathbb{Q}(i), \quad x \in \mathbf{Z}_5 \tag{5.1}$$

and show that it has no solution there. We take the valuations of both sides of (5.1)

$$\nu_5(a^2 - 5b^2) = \nu_5(2 + 5x)$$

to show that a and b must be in $\mathbf{Z}_5$. In fact, since $x \in \mathbf{Z}_5$, $\nu_5(2 + 5x) \geq \min\{\nu_5(2), \nu_5(x) + 1\} = 0$, and we have equality as both valuations are distinct. Now, $\nu_5(a^2 - 5b^2) = \min\{2\nu_5(a), 2\nu_5(b) + 1\}$ must be 0, hence $\nu_5(a) = 0$ which implies $a \in \mathbf{Z}_5$ and thus $b \in \mathbf{Z}_5$.

We conclude by showing that

$$a^2 - 5b^2 = 2 + 5x \ a, b, x \in \mathbf{Z}_5$$

has no solution. Reducing modulo $5\mathbf{Z}_5$ we find that 2 should be a square in the finite field $GF(5)$, which is a contradiction. □

5.2.2 The Lattice $\mathbb{Z}[i]^2$

Let us see now how to add the shaping property on the codebook built on $\mathcal{A}$. Equation (4.5) tells us that

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{5})}| = 5|N_{L/K}(\alpha)|^2.$$

We thus look for an element α such that $|N_{L/K}(\alpha)|^2 = 5$. In order to find such an element, we look at the factorization of 5 in $\mathcal{O}_L$:

$$5 = (1 + i - i\theta)^2(1 - i + i\theta)^2.$$

We thus choose $\alpha = 1 + i - i\theta$. Let us now check that we indeed get the right lattice. Its generator matrix is given by

$$M = \begin{pmatrix} \alpha & \alpha\theta \\ \sigma(\alpha) & \sigma(\alpha\theta) \end{pmatrix}.$$

A direct computation shows that $MM^\dagger = 5\mathbf{I}_2$. Thus $\frac{1}{\sqrt{5}}M$ is a unitary matrix, yielding the shaping property.

A codeword $\mathbf{X}$ belonging to the Golden code has thus, adding the shaping property, the form:

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ i\sigma(\alpha)(c+d\sigma(\theta)) & \sigma(\alpha)(a+b\sigma(\theta)) \end{bmatrix},$$

where a, b, c, d are QAM symbols.

Recall that when a, b, c, d can take any value in $\mathbb{Z}[i]$, we say that we have an *infinite code* $\mathcal{C}_\infty$. This terminology recalls the case where finite signal constellations are carved from infinite lattices.

5.2.3 The Minimum Determinant

Let us now compute the minimum determinant of the infinite code. Since $\alpha\sigma(\alpha) = 2 + i$, we have

$$\begin{aligned} \det(\mathbf{X}) &= \frac{2+i}{5}[(a+b\theta)(a+b\sigma(\theta)) - i(c+d\theta)(c+d\sigma(\theta))] \\ &= \frac{1}{2-i}[(a^2+ab-b^2-i(c^2+cd-d^2)]. \end{aligned}$$

By definition of a, b, c, d, we have that the non-trivial minimum of $|a^2+ab-b^2-i(c^2+cd-d^2)|^2$ is 1, thus

$$\delta_{\min}(\mathcal{C}_\infty) = \min_{\mathbf{0}\neq\mathbf{X}\in\mathcal{C}} |\det(\mathbf{X})|^2 = \frac{1}{5}.$$

Thus the minimum determinant of the infinite code is bounded away from zero, as required.

Since an explicit computation of the determinant will not be possible in higher dimension, we show now another way of computing the minimum determinant. Since

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} a+b\theta & c+d\theta \\ i(c+d\sigma(\theta)) & a+b\sigma(\theta) \end{bmatrix},$$

we have that

$$\min_{\mathbf{X}\neq\mathbf{0}} \det(\mathbf{X}) = \frac{1}{5} N_{L/K}(\alpha) \min_{\mathbf{X}\neq\mathbf{0}} \det \begin{bmatrix} a+b\theta & c+d\theta \\ i(c+d\sigma(\theta)) & a+b\sigma(\theta) \end{bmatrix}.$$

Using Theorem 4.7, the determinant on the right-hand side is lower bounded by 1. Thus

$$\min_{\mathbf{X}\neq\mathbf{0}} |\det(\mathbf{X})|^2 = \frac{1}{25}|N_{L/K}(\alpha)|^2 = \frac{1}{5}$$

since α has been chosen such that $|N_{L/K}(\alpha)|^2 = 5$.

Note in the second row of the codeword $\mathbf{X}$ the factor i, which guarantees uniform average transmitted energy since $|i|^2 = 1$.

5.3 A Perfect STBC for 3 Antennas

For 3 antennas, we use HEX symbols. Thus, the base field is $K = \mathbb{Q}(j)$. Let $\theta = \zeta_7 + \zeta_7^{-1} = 2\cos(\frac{2\pi}{7})$ and $L = \mathbb{Q}(j,\theta)$, the compositum of K and $\mathbb{Q}(\theta)$. We have $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$, and thus $[\mathbb{Q}(j,\theta) : K] = 3$. The discriminant of $\mathbb{Q}(\theta)$ is $d_{\mathbb{Q}(\theta)} = 49$, the minimal polynomial $p_\theta(X) = X^3 + X^2 - 2X - 1$. The extension L/K is cyclic with generator $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$.

We consider the cyclic algebra $\mathcal{A} = (L/K, \sigma, j)$ of degree 3, that is

$$\mathcal{A} = L \oplus eL \oplus e^2L$$

with $e \in \mathcal{A}$ such that $e^3 = j$ and $\lambda e = e\sigma(\lambda)$ for all $\lambda \in L$. The choice of $\gamma = j$ yields a perfect code. Since j and j^2 are not norms in L/K [44], the code is fully diverse.

5.3.1 The Lattice $\mathbb{Z}[j]^3$

Since we use HEX symbols, we look for a $\mathbb{Z}[j]$-lattice which is a rotated $\mathbb{Z}[j]^3 (= A_2^3)$ lattice. Equation (4.5) tells us that

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{\theta})}| = 7^2 |N_{L/K}(\alpha)|^2.$$

A necessary condition to obtain a rotated $\mathbb{Z}[j]^3$ lattice is thus the existence of an element α such that $|N_{L/K}(\alpha)|^2 = 7$. Let us look at the factorization of 7 in $\mathcal{O}_L$:

$$7 = ((1+j)+\theta)^3 \overline{((1+j)+\theta)}^3.$$

Let us take $\alpha = (1+j)+\theta$. A $\mathbb{Z}[j]$-basis of $(\alpha)\mathcal{O}_L$ is given by $\{\alpha\theta^k\}_{k=0}^2 = \{(1+j)+\theta, (1+j)\theta+\theta^2, 1+2\theta+j\theta^2\}$. Using the

change of basis given by the following matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 2 & 1 & 0 \end{pmatrix},$$

one gets a reduced $\mathbb{Z}[j]$-basis

$$\begin{aligned}\{\nu_k\}_{k=1}^{3} = \{&(1+j)+\theta, (-1-2j)+j\theta^2, (-1-2j) \\ &+(1+j)\theta+(1+j)\theta^2\}.\end{aligned}$$

Then by straightforward computation we find

$$\frac{1}{7}\mathrm{Tr}_{L/\mathbb{Q}(j)}(\nu_k\bar{\nu_l}) = \delta_{kl} \quad k,l = 1,2,3$$

using $\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = 3,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = -1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 5.$

We compute, for example, the diagonal coefficients

$$\mathrm{Tr}_{L/\mathbb{Q}(j)}(\nu_k\bar{\nu_k}) = \begin{cases} \mathrm{Tr}_{L/\mathbb{Q}(j)}(1+\theta+\theta^2) = 7 & \text{if } k = 1 \\ \mathrm{Tr}_{L/\mathbb{Q}(j)}(2-\theta) = 7 & \text{if } k = 2 \\ \mathrm{Tr}_{L/\mathbb{Q}(j)}(4-\theta^2) = 7 & \text{if } k = 3 \end{cases}$$

The generator matrix of the lattice in its numerical form is thus given by

$$\begin{aligned} M &= \tfrac{1}{\sqrt{7}}(\sigma_l(\nu_k))_{k,l=1}^{n} \\ &= \begin{pmatrix} 0.66030 + 0.32733i & 0.02077 + 0.32733i & -0.49209 + 0.32733i \\ -0.29386 - 0.14567i & -0.03743 - 0.58982i & -0.61362 + 0.40817i \\ 0.52952 + 0.26250i & -0.04667 - 0.73550i & 0.27309 - 0.18165i \end{pmatrix}. \end{aligned}$$

A codeword $\mathbf{X} \in \mathcal{C}$ encodes nine HEX symbols $x_0, \ldots, x_9$ as

$$\mathbf{X} = \sum_{k=0}^{2} \mathrm{diag}\left(M(x_{3k}, x_{3k+1}, x_{3k+2})^T\right) E^k,$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma & 0 & 0 \end{pmatrix}.$$

5.3.2 The Minimum Determinant

Using the argument described in Subsection 5.2.3, we have

$$\delta_{\min}(\mathcal{C}) = \frac{1}{7^3}|N_{L/\mathbb{Q}(j)}(\alpha)|^2 = \frac{7}{7^3}$$

by choice of α. Thus the minimum determinant is given by

$$\delta_{\min}(\mathcal{C}) = \frac{1}{49}.$$

5.4 A Perfect STBC for 4 Antennas

As for the Golden code, we consider the transmission of QAM symbols, thus, the base field is $K = \mathbb{Q}(i)$. Let $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos(\frac{2\pi}{15})$ and $L = \mathbb{Q}(i,\theta)$, the compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\theta)$. We have $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$, and thus $[\mathbb{Q}(i,\theta) : \mathbb{Q}(i)] = 4$. The discriminant of $\mathbb{Q}(\theta)$ is $d_{\mathbb{Q}(\theta)} = 1125$ and the minimal polynomial $p_\theta(X) = X^4 - X^3 - 4X^2 + 4X + 1$. The extension $L/\mathbb{Q}(i)$ is cyclic with generator $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$.

The corresponding cyclic algebra of degree 4 is given by $\mathcal{A} = (L/K, \sigma, i)$, that is

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus e^3L$$

with $e \in L$ such that $e^4 = i$ and $\lambda e = e\sigma(\lambda)$ for all $\lambda \in L$. The choice of $\gamma = i$ yields a perfect code. Since $\pm i$ and -1 are not norms in L/K [44], the code is fully diverse.

5.4.1 The Lattice $\mathbb{Z}[i]^4$

We search for a complex rotated lattice $\mathbb{Z}[i]^4$. Using Equation (4.5), we have

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{\theta})}| = 3^2 5^3 |N_{L/K}(\alpha)|^2.$$

A necessary condition to obtain a rotated version of $\mathbb{Z}[i]^4$ is that there exists an element α such that $|N_{L/K}(\alpha)|^2 = 3^2 5$. Let us look at the factorization of 3 and 5 in $\mathcal{O}_L$:

$$\begin{aligned} 3 &= (\alpha_3)^2 \overline{(\alpha_3)}^2 \\ 5 &= (\alpha_5)^4 \overline{(\alpha_5)}^4. \end{aligned}$$

Let us consider $\alpha = \alpha_3\alpha_5 = (1-3i) + i\theta^2$.

A $\mathbb{Z}[i]$-basis of (α) is given by $\{\alpha\theta^i\}_{i=0}^3$. Using the change of basis given by the following matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix},$$

one gets a new $\mathbb{Z}[i]$-basis

$$\begin{aligned}\{\nu_k\}_{k=1}^4 = \{&(1-3i) + i\theta^2, (1-3i)\theta + i\theta^3, \\ &-i + (-3+4i)\theta + (1-i)\theta^3, (-1+i) - 3\theta + \theta^2 + \theta^3\}.\end{aligned}$$

Then by straightforward computation we can check that

$$\frac{1}{15}\mathrm{Tr}_{L/\mathbb{Q}(i)}(\nu_k\bar{\nu_\ell}) = \delta_{k\ell} \quad k,\ell = 1,\ldots,4$$

using

$$\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 9,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = 1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = 29.$$

For example, we compute the diagonal coefficients,

$$\mathrm{Tr}_{L/\mathbb{Q}(i)}(|\nu_k|^2) = \begin{cases} \mathrm{Tr}_{L/\mathbb{Q}(i)}(10 - 6\theta^2 + \theta^4) = 15 & \text{if } k = 1 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(1 + 3\theta + \theta^2 - \theta^3) = 15 & \text{if } k = 2 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(5 + 6\theta - \theta^2 - 2\theta^3) = 15 & \text{if } k = 3 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(-5\theta + 2\theta^2 + 2\theta^3) = 15 & \text{if } k = 4 \end{cases}.$$

The unitary generator matrix of the lattice is given by

$$\begin{aligned} M &= \frac{1}{\sqrt{15}}(\sigma_\ell(\nu_k))_{k,\ell=1}^n \\ &= \begin{pmatrix} 0.258 - 0.312i & 0.346 - 0.418i & -0.418 + 0.505i & -0.214 + 0.258i \\ 0.258 + 0.087i & 0.472 + 0.160i & 0.160 + 0.054i & 0.763 + 0.258i \\ 0.258 + 0.214i & -0.505 - 0.418i & -0.418 - 0.346i & 0.312 + 0.258i \\ 0.258 - 0.763i & -0.054 + 0.160i & 0.160 - 0.472i & -0.087 + 0.258i \end{pmatrix}. \end{aligned}$$

A codeword $\mathbf{X} \in \mathcal{C}$ encodes 16 QAM symbols $x_0,\ldots,x_{15}$ so that $\mathbf{X} \in \mathcal{C}$ is given by

$$\mathbf{X} = \sum_{k=0}^{3} \mathrm{diag}\left(M(x_{4k}, x_{4k+1}, x_{4k+2}, x_{4k+3})^T\right) E^k,$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 \end{pmatrix}.$$

5.4.2 The Minimum Determinant

Using the argument of Subsection 5.2.3, the minimum determinant of the infinite code is equal to

$$\delta_{\min}(\mathcal{C}) = \frac{1}{15^4}|N_{L/\mathbb{Q}(i)}(\alpha)|^2 = \frac{45}{15^4}$$

by choice of α. Thus the minimum determinant is given by

$$\delta_{\min}(\mathcal{C}) = \frac{1}{1125}.$$

5.5 A Perfect STBC for 5 Antennas

For the 5 antennas case, we present the construction of [21], which transmits QAM symbols. Thus, the base field is $K = \mathbb{Q}(i)$. Let $\theta = \zeta_{11} + \zeta_{11}^{-1} = 2\cos(\frac{2\pi}{11})$ and $L = \mathbb{Q}(i,\theta)$, the compositum of K and $\mathbb{Q}(\theta)$. We have $[\mathbb{Q}(\theta) : \mathbb{Q}] = 5$, and thus $[\mathbb{Q}(j,\theta) : K] = 5$. The extension L/K is cyclic with generator $\sigma : \zeta_{11} + \zeta_{11}^{-1} \mapsto \zeta_{11}^2 + \zeta_{11}^{-2}$.

The corresponding cyclic algebra of degree 5 is $\mathcal{A} = (L/K, \sigma, \gamma)$, that is

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus e^3L \oplus e^4L$$

with $e \in \mathcal{A}$ such that $e^5 = \gamma \in K$, $\gamma \neq 0$ and $\lambda e = e\sigma(\lambda)$ for all $\lambda \in L$. In order to obtain a division algebra, γ is chosen in [21] to be

$$\gamma = \frac{3+2i}{2+3i}.$$

Note here that γ is not a root of unity, but is of the form an element of K divided by its complex conjugate, which makes it of norm 1. That this γ yields a division algebra has been shown in [21]. This way of finding a suitable non-norm element γ of norm 1 has been used more generally in [21] to find codes in arbitary dimensions.

5.5.1 The Lattice $\mathbb{Z}[i]^5$

Finding the $\mathbb{Z}[i]^5$ lattice now uses a different, more elaborated technique, which has been presented in [4, 21], to which we let the interested reader refer. The generator matrix M is numerically given by

$$M = \begin{pmatrix} -0.3260 & 0.5485 & -0.4557 & -0.5969 & -0.1699 \\ 0.5485 & -0.4557 & -0.5969 & -0.1699 & -0.3260 \\ -0.4557 & -0.5969 & -0.1699 & -0.3260 & 0.5485 \\ -0.5969 & -0.1699 & -0.3260 & 0.5485 & -0.4557 \\ -0.1699 & -0.3260 & 0.5485 & -0.4557 & -0.5969 \end{pmatrix}.$$

A codeword $\mathbf{X} \in \mathcal{C}$ encodes 25 QAM symbols $x_0, \ldots, x_{24}$ so that $\mathbf{X} \in \mathcal{C}$ is given by

$$\mathbf{X} = \sum_{k=0}^{4} \mathrm{diag}\left(M(x_{5k}, x_{5k+1}, x_{5k+2}, x_{5k+3}, x_{5k+4})^T\right) E^k,$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 & 0 \end{pmatrix}.$$

5.5.2 The Minimum Determinant

The code construction being here a bit different than the previous examples yields a different computation for the minimum determinant. First, the argument of Subsection 5.2.3 has to be slightly modified. We have that

$$\det(\mathbf{X}) = \det \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \\ \gamma\sigma(x_4) & \sigma(x_0) & \sigma(x_1) & \sigma(x_2) & \sigma(x_3) \\ \gamma\sigma^2(x_3) & \gamma\sigma^2(x_4) & \sigma^2(x_0) & \sigma^2(x_1) & \sigma^2(x_2) \\ \gamma\sigma^3(x_2) & \gamma\sigma^3(x_3) & \gamma\sigma^3(x_4) & \sigma^3(x_0) & \sigma^3(x_1) \\ \gamma\sigma^4(x_1) & \gamma\sigma^4(x_2) & \gamma\sigma^4(x_3) & \gamma\sigma^4(x_4) & \sigma^4(x_0) \end{pmatrix}$$

$$= \frac{1}{\gamma_d^4} \det \underbrace{\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \\ \gamma_n\sigma(x_4) & \sigma(x_0) & \sigma(x_1) & \sigma(x_2) & \sigma(x_3) \\ \gamma_n\sigma^2(x_3) & \gamma_n\sigma^2(x_4) & \sigma^2(x_0) & \sigma^2(x_1) & \sigma^2(x_2) \\ \gamma_n\sigma^3(x_2) & \gamma_n\sigma^3(x_3) & \gamma_n\sigma^3(x_4) & \sigma^3(x_0) & \sigma^3(x_1) \\ \gamma_n\sigma^4(x_1) & \gamma_n\sigma^4(x_2) & \gamma_n\sigma^4(x_3) & \gamma_n\sigma^4(x_4) & \sigma^4(x_0) \end{pmatrix}}_{\tilde{\mathbf{x}}},$$

where $\gamma_n = 3 + 2i$ and $\gamma_d = 2 + 3i$ are, respectively, the numerator and the denominator of γ. Thus, we have that

$$\min |\det(\mathbf{X})|^2 = \frac{1}{|\gamma_d^4|^2} \min |\det(\tilde{\mathbf{X}})|^2.$$

Since $\tilde{\mathbf{X}}$ is now a matrix with coefficients in $\mathbb{Z}[i]$, the explanation of Subsection 5.2.3 holds for $\tilde{\mathbf{X}}$, namely

$$\min |\det(\tilde{\mathbf{X}})|^2 = \frac{1}{11^5} |N_{L/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{11^4},$$

where α has been found as explained in [4, 21], so that finally

$$\delta_{\min}(\mathcal{C}) = \frac{1}{11^4 13^4} = \frac{1}{143^4}$$

since $|\gamma_d^4|^2 = (|2 + 3i|^2)^4$.

5.6 A Perfect STBC for 6 Antennas

As in the 3 antennas case, we transmit HEX symbols. Thus, the base field is $K = \mathbb{Q}(j)$. Let $\theta = \zeta_{28} + \zeta_{28}^{-1} = 2\cos(\frac{\pi}{14})$ and $L = \mathbb{Q}(j, \theta)$, the compositum of K and $\mathbb{Q}(\theta)$. We have $[\mathbb{Q}(\theta) : \mathbb{Q}] = 6$, and thus $[\mathbb{Q}(j, \theta) : K] = 6$. The extension L/K is cyclic with generator $\sigma : \zeta_{28} + \zeta_{28}^{-1} \mapsto \zeta_{28}^2 + \zeta_{28}^{-2}$.

The corresponding cyclic algebra of degree 6 is $\mathcal{A} = (L/K, \sigma, \gamma)$, that is

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus e^3L \oplus e^4L \oplus e^5L$$

with $e \in \mathcal{A}$ such that $e^6 = \gamma \in K$, $\gamma \neq 0$ and $\lambda e = e\sigma(\lambda)$ for all $\lambda \in L$. In order to obtain a perfect code, we choose $\gamma = -j$. Since γ and its powers are not norms in L/K [44], the code is fully diverse.

5.6.1 The Lattice $\mathbb{Z}[j]^6$

In order to find the $\mathbb{Z}[j]^6$ lattice, we use Equation (4.5):

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{\theta})}| = 2^6 7^5 |N_{L/K}(\alpha)|^2.$$

A necessary condition to obtain a rotated version of $\mathbb{Z}[j]^6$ is that there exists an element α such that $|N_{L/K}(\alpha)|^2 = 7$. Similarly as before, we start by looking at the factorization of 7 in $\mathcal{O}_L$. However, unlike previously, we cannot write $7 = (\alpha_7)^6 \overline{(\alpha_7)}^6$. Such factorization does not exist. We thus consider the principal ideal $(7)\mathcal{O}_L$, and look at its factorization [44, 48]

$$(7)\mathcal{O}_L = \mathcal{I}_7^6 \overline{\mathcal{I}_7}^6.$$

The factorization of $(7)\mathcal{O}_L$ is given as a product of *non-principal* ideals. This makes harder the explicit computation of an ideal basis, and in particular of the ideal basis (if any) for which the Gram matrix becomes the identity.

We thus compute numerically a basis of $\mathcal{I}_7$, from which we compute a Gram matrix of the lattice. We then perform a basis reduction on the Gram matrix, using an LLL reduction algorithm [44]. We get the following change of basis

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1+j & 0 & 1 & 0 & 0 & 0 \\ -1-2j & 0 & -5 & 0 & 1 & 0 \\ 1+j & 0 & 4 & 0 & -1 & 0 \\ 0 & -3 & 0 & 1 & 0 & 0 \\ 0 & 5 & 0 & -5 & 0 & 1 \end{pmatrix}$$

and the lattice generator matrix in numerical form: $M = \frac{1}{\sqrt{14}}\tilde{M}$ where $\tilde{M}$ is given by

$$\begin{pmatrix} 1.9498 & 1.3019-0.87i & -0.0549-0.87i & -1.7469-0.87i & 1.5636 & 0.8677 \\ 0.8677 & -1.7469-0.87i & 1.3019-0.87i & -0.0549-0.87i & -1.9498 & 1.5636 \\ 1.5636 & -0.0549-0.87i & -1.7469-0.87i & 1.3019-0.87i & -0.8677 & -1.9498 \\ -1.9498 & 1.3019-0.87i & -0.0549-0.87i & -1.7469-0.87i & -1.5636 & -0.8677 \\ -0.8677 & -1.7469-0.87i & 1.3019-0.87i & -0.0549-0.87i & 1.9498 & -1.5636 \\ -1.5636 & -0.0549-0.87i & -1.7469-0.87i & 1.3019-0.87i & 0.8677 & 1.9498 \end{pmatrix}.$$

This matrix $MM^\dagger$ is the identity matrix, so that we indeed get a rotated version of the A_2^6 lattice.

A codeword $\mathbf{X} \in \mathcal{C}$ encodes 36 HEX symbols $x_0, \ldots, x_{35}$ so that $\mathbf{X} \in \mathcal{C}$ is given by

$$\mathbf{X} = \sum_{k=0}^{5} \mathrm{diag}\left(M(x_{6k}, x_{6k+1}, x_{6k+2}, x_{6k+3}, x_{6k+4}, x_{6k+5})^T\right) E^k,$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

5.6.2 The Minimum Determinant

Since the ideal $\mathcal{I}_7$ is not principal, we do not know how to compute the minimum determinant. We thus use the bounds given in [44]:

$$\frac{1}{2^6 7^5} \leq \delta_{\min}(\mathcal{C}_\infty) \leq \frac{1}{2^6 7^4}.$$

5.7 Optimality of Perfect STBCs

Let us first consider the case of 2×2 perfect STBCs. In [44], an infinite family of 2×2 perfect STBCs is given. Since all those codes are perfect, they are only distinguishable by their minimum determinant, which in this case is given by $1/p$, where p is a prime number such that $p \equiv 5 \pmod 8$. Since the Golden code uses $p = 5$, it is the best. Let us now address the question of the optimality of the Golden code more generally, that is, without restricting ourselves to this family parameterized by $p \equiv 5 \pmod 8$. Using Equation (4.5) and the fact that we encode a perfect STB code using a lattice $\Lambda = \mathbb{Z}[i]^2$ such that $\det(\Lambda) = 1$, we have

$$1 = |N_{L/\mathbb{Q}(i)}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{d})}|,$$

Table 5.1 Summarizing the known discriminants of perfect STBCs.

n	disc
2	5
3	49
4	1125
5	143^4
6	$2^6 7^5$

so that the minimum determinant of a 2×2 perfect code is

$$\delta_{\min}(\mathcal{C}_\infty) = \frac{1}{d_{\mathbb{Q}(\sqrt{d})}},$$

where $d_{\mathbb{Q}(\sqrt{d})}$ denote the discriminant of a quadratic field $\mathbb{Q}(\sqrt{d})$. That no quadratic number field can yield both a smaller discriminant and a cyclic division algebra has been proven in [41].

A different approach to improve on the Golden code has started in [31], where the authors investigate maximal orders of algebras.

In higher dimensions, the only available code constructions are those from [21, 44]. Though it is clear that taking for γ a root of unity yields a better coding gain, the question of finding perfect STB codes with better coding gain stays open. Using again (4.5), the minimum determinant of a perfect STB code in general is related to discriminant of L/K. A formulation of the optimality of perfect codes in higher dimensions could be addressed in finding number fields L/K with smaller discriminant than those known which furthermore yield the other properties of division algebra and shaping. Table 5.1 summarizes the best known discriminants so far.

6

New Applications and Conclusion

In this last chapter, we briefly outline further research directions involving perfect STBCs, namely generalization to wireless networks and applications to coded modulations.

6.1 Coding for Wireless Networks

A lot of attention has been paid recently to wireless networks. Coding strategies for wireless networks proposed so far (for example see [34]) have been looking for methods to exploit spatial diversity using the antennas of different users in the network. The idea is to have the nodes forming a virtual antenna array, to obtain the diversity known to be achieved by point-to-point MIMO systems. Such coding strategies have been called *cooperative diversity* schemes.

Different families of coding strategies have been proposed. They are mainly classified between *Amplify-and-Forward* protocols, and *Decode-and-Forward* protocols. Both protocols comprise a two-step transmission: first a broadcast phase, where the transmitter broadcasts his message to the neighbor relay nodes. In the amplify-and-forward protocol, relay nodes receive the signal, just amplify it, and in a second

phase, forward the amplified version to the receiver. In the decode-and-forward protocol, relay nodes try to decode the received signal, and those which manage then forward the decoded signal to the receiver. The second phase of those protocols is usually a phase of cooperation, since both these two protocols can be improved by having the nodes cooperating in doing some encoding before sending the signal to the receiver. In the decode-and-forward case, relays which decoded can cooperate in re-encoding a Space–Time code [16, 34]. In the amplify-and-forward case, a way of getting cooperation is to use *distributed Space–Time coding* [35], as we detail below.

6.1.1 Distributed Space–Time coding

The following two-step protocol, which can be seen as an improved amplify-and-forward protocol, has been introduced in [35]. We report here the basic idea of the protocol, ignoring on purpose normalization factors. All random variables for noise and fading are assumed to be complex Gaussian with zero mean and unit variance. The transmitter sends its signal $\mathbf{s}$ to each relay which can sense it, so that the ith relay gets

$$\mathbf{r}_i = f_i \mathbf{s} + \mathbf{v}_i,$$

where $\mathbf{v}_i$ is the noise vector and f_i is the fading at the ith relay. Now each relay transmits

$$\mathbf{t}_i = A_i \mathbf{r}_i,$$

where A_i is a unitary matrix, so that the receiver gets

$$\mathbf{x} = \sum_{i=1}^{R} g_i \mathbf{t}_i + \mathbf{w} = SH + W,$$

with

$$S = [A_1\mathbf{s} \cdots A_R\mathbf{s}], \quad H = \begin{bmatrix} f_1 g_1 \\ \vdots \\ f_R g_R \end{bmatrix} \tag{6.1}$$

and

$$W = \sum_{i=1}^{R} g_i A_i \mathbf{v}_i + \mathbf{w}.$$

The matrix S is called a *distributed Space–Time code* since it has been generated in a distributed way by the relay nodes. It has been shown in [35] by analyzing the behavior of the pairwise error probability that the rank criterion holds similarly to the point-to-point case.

Thus knowledge acquired for building Space–Time codes is useful for coding for wireless networks. Adaptation of perfect Space–Time codes have been used for wireless networks for example in [19, 37, 42]. Furthermore, since in wireless networks, the number of relay nodes correspond to the number of antennas, it is useful to have general code constructions, as given in [21].

6.1.2 MIMO Amplify-and-Forward Protocol

While the work discussed in the previous subsection focused on the analysis of the pairwise probability of error as design criterion, a lot of work has been done using as criterion the diversity-multiplexing gain trade-off (DMT) described in Chapter 3. In [2], the amplify-and-forward protocol has been analyzed with respect to the DMT. Note that the network model considered assume a direct link from the transmitter link to the receiver link, unlike the distributed Space–Time code model. It was shown that in order to reach the trade-off, the protocol has to be such that the transmitter node always transmits, which yields to so-called *non-orthogonal amplify-and-forward* protocol. In [2], the DMT has been shown to be achieved using random Gaussian codebooks. Since perfect Space–Time codes achieve the DMT in the point-to-point case, they seem natural candidates to generalize in order to reach the trade-off in the relay case. This has been proposed in [62], where the protocol has further been extended to the case of relays equipped with multiple antennas.

6.2 Trellis/Block Coded Modulations

Wireless networks for multimedia traffic demand high spectral efficiency coding schemes with low packet delay. Perfect Space–Time codes

provide some very good tools to solve this challenging design problem. Wireless channels are commonly modeled as *slow block fading*, i.e., the channel coefficients are fixed over the duration of a frame. The careful concatenation of a Space–Time block code with an outer trellis code provides a robust solution for high rate transmission over a slow block fading channel.

In [32], a concatenated scheme is considered, where the inner code is the Golden code and the outer code is a trellis code. We can view this as a multidimensional trellis coded modulation (TCM), where the Golden code acts as a signal set to be partitioned. This *Golden Space–Time Trellis Coded Modulation* (GST-TCM) scheme is appropriate for high data rate systems thanks to the great flexibility in the choice of the modulation spectral efficiency. Moreover, the ML decoder complexity remains independent of the frame length.

A first attempt to design such a scheme was made in [10]. However, the resulting *ad hoc* scheme suffered from a high trellis complexity. In [32], a systematic design approach for GST-TCM over slow block fading channels was based on lattice set partitioning combined with a trellis code is used to increase the minimum determinant between codewords. The Viterbi algorithm is used for trellis decoding, where the branch metrics are computed using a sphere decoder for the inner code.

The different GST-TCM codes designed in [32] were searched using the standard Ungerboeck's design rules for TCM. For example, it is shown that a 16 state TCM, with the spectral efficiency of 6 bits per channel use (bpcu), achieves a significant performance gain of 4.2 dB over the uncoded Golden code in slow and fast block fading channels, at an frame error rate (FER) of 10^{-3}.

A natural research direction is to extend those techniques to other perfect Space–Time codes.

6.3 Other Issues

There are other recent extensions and developments of the applications of cyclic division algebras to the area of wireless communications. One of the most promising extensions is by using maximal orders of the algebra in order to have a larger set of codewords with at least

the same minimum determinant [30]. There are also other applications for division algebras based codes than the MIMO or the Relay channel such as, for instance, the MIMO-ARQ channel [47].

6.4 Conclusion

Designing efficient Space–Time codes for coherent MIMO systems involve more than fulfilling the known rank and determinant criteria. In this paper, we detailed several other parameters to take into account to optimize the efficiency of Space–Time codes, such as constellation shaping, diversity-multiplexing gain trade-off and the information lossless property. In order to actually construct codes satisfying those constraints, we heavily rely on the algebraic structure of cyclic division algebras based on number fields. In order to make those division algebra based codes accessible, we provide a self-contained introduction to the algebraic techniques involved. In some sense, those are a generalization of previous methods used for single antenna coding, and we believe that these algebraic approaches are now very promising for facing new coding problems coming from wireless networks.

Acknowledgments

This work was supported in part by the STREP project No. IST-026905 (MASCOT) within the Sixth Framework Program of the European Commission.

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.