Signal Space Diversity:
a power and bandwidth efficient
diversity technique for the Rayleigh fading channel

J. Boutros*, E. Viterbo†

Abstract

The increasing need of high data rate transmissions over time or frequency selective fading channels has drawn attention to modulation schemes with high spectral efficiency such as QAM. With the aim of increasing the 'diversity order' of the signal set we consider the multidimensional rotated QAM constellations. Very high diversity orders can be achieved and this results in an almost Gaussian performance over the fading channel. This multidimensional modulation scheme is essentially uncoded and enables to trade diversity for system complexity, at no expense of power or bandwidth.

Key Words : QAM Modulation, fading, diversity, number fields, rotation, lattices.

I. Introduction

The rapidly growing need of high data rate transmissions over fading channels has stimulated the interest for AM-PM modulation schemes with high spectral efficiency (or throughput) [1], [2], [3]. The effectiveness of these transmission schemes basically relies on the good error correcting capabilities of a code. The price to pay for this gain is either a bandwidth expansion or an additional transmission power to accommodate the redundant bits.

In this paper we present a different approach. We consider uncoded multidimensional modulation schemes with an intrinsic *diversity order*, which achieve substantial coding gains over fading channels. The *diversity order* of a multidimensional signal set is the minimum number of distinct components between any two constellation points. In other words, the diversity order is the minimum Hamming distance between any two coordinate vectors of

*Ecole Nationale Supérieure des Télécommunications, 46, rue Barrault, 75634 Paris Cedex 13, France

†Politecnico di Torino, C. Duca degli Abruzzi 24, I-10129 Torino, Italy

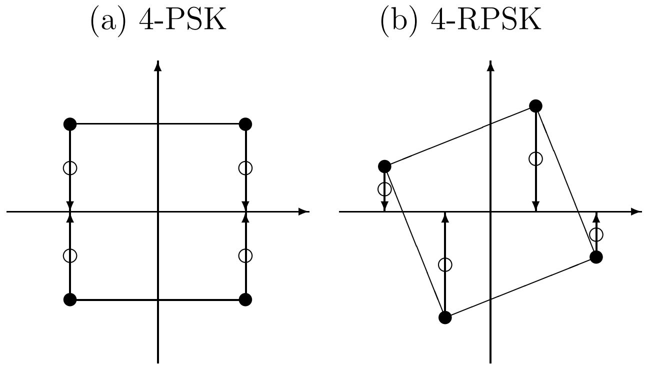

Fig. 1. How to increase diversity: (a) $L = 1$, (b) $L = 2$.

constellation points.

To distinguish from other well known types of diversity (time, frequency, space, code) we will talk about *modulation diversity* or *signal space diversity.* Throughout the paper we will use, for simplicity, only the term *diversity* and it will be denoted with the symbol L.

As we will show in the following, the key point to increase the modulation diversity is to apply a certain rotation to a classical signal constellation in such a way that any two points achieve the maximum number of distinct components. Figure 1 illustrates this idea on a 4-PSK. In fact, if we suppose that a deep fade hits only one of the components of the transmitted signal vector, then we can see that the 'compressed' constellation in (b) (empty circles) offers more protection against the effects of noise, since no two points collapse together as would happen with (a). A component interleaver/deinterleaver pair is required to assume that the in-phase and quadrature components of the received symbol are affected by independent fading. This simple operation already results in a gain of $8\,dB$ at 10^{-3} over the traditional 4-PSK (see Fig. 11). We will show in this paper, that the increase in the dimensionality of the signal set produces significant gains in a fading channel, over the corresponding non-rotated signal set.

An interesting feature of the rotation operation is that the rotated signal set has exactly the same performance of the non rotated one when used over a pure AWGN channel. The rotated constellation when used over a Ricean fading channel will show a performance between the two extreme cases of Gaussian and Rayleigh fading channel.

We have used the term 'uncoded' since we are not adding any type of redundancy to the information bit stream. The information bits are grouped into blocks and directly mapped one-to-one onto the multidimensional constellation points. This means that the coding gain is obtained without spending additional power or bandwidth, but only increasing the complexity of the demodulation operation. In fact, demodulation must now be performed on blocks of consecutive symbols.

The scope of this paper is to analyze in detail all the methods devised to construct high diversity multidimensional QAM constellations carved from a rotated cubic lattice Z^n.

Most of the best known lattices for the Gaussian channel have the property of being integral, i.e. subsets of the cubic lattice Z^n, so this can be used to obtain convenient labelings. In the case of Rayleigh fading channel, no efficient labeling was found for the optimal lattices given in [4], thus limiting their practical use. The rotated multidimensional QAM constellations presented in this paper can be easily labeled by Gray mapping.

The paper is structured as follows. Sections II and III introduce the system model and review some elementary concepts of algebraic number theory. In Section IV it is proved that for large values of diversity the point error probability over a fading channel approaches the one over an AWGN channel. This property is verified through simulation and for values of modulation diversity larger than 12, the bit error rate curves are within 1-2dB from the corresponding Gaussian curve. Section V presents three different techniques we used to increase the diversity of multidimensional QAM-type signal constellations. Although the most important, diversity is not the only parameter which influences the system performance. It is also important to maximize the *minimum product distance* between any two points of the signal constellation. This problem is considered in Section VI. Finally we give our results and conclusions in Sections VII and VIII respectively.

II. The multidimensional QAM system

We now describe the system model shown in Figure 2. An n-dimensional QAM constellation is obtained as the Cartesian product of $n/2$ two-dimensional QAM signal sets. A block of m bits is mapped onto the constellation by applying the Gray mapping in each dimension.

We obtain an overall Gray mapping which results in a one bit change when moving from one constellation point to any one of its nearest neighbors.

Each group of m/n bits uniquely identifies one of the n components of the multidimensional QAM constellation vector $\mathbf{u} = (u_1, \dots u_n)$, where $u_i = \pm 1, \pm 3, \dots$. We will call $\mathbf{u}$ the *integer component vector*. We denote by η the system throughput measured as the number of bits per symbol (two dimensions), so we have $m = \eta n/2$. In the case of odd dimension, one of the symbols should be split between two successive points. The total number of points in this cubic shaped constellations is 2^m and the average energy per bit is simply $E_b = (2^\eta - 1)/3\eta$.

We can view this constellation as carved from a translated and scaled (enlarged by a factor 2) version of the n-dimensional cubic lattice Z^n. In the following, for simplicity, we will consider only the constellations carved form Z^n, so that $u_i = 0, \pm 1, \pm 2, \dots$. By simple scaling and translation it is possible to revert to the multidimensional QAM constellation.

The point $\mathbf{x}$ of the rotated constellation is obtained by applying the rotation matrix M to $\mathbf{u}$. The set of all points $\{\mathbf{x} = \mathbf{u}M, \mathbf{u} \in Z^n\}$ belongs to the n-dimensional cubic lattice $Z_{n,L}$ with generator matrix M and diversity L. The two lattices Z^n and $Z_{n,L}$ are equivalent in the sense of Section V-A, but exhibit a different modulation diversity. In the following we will identify the lattice with the corresponding finite constellation carved from the lattice.

The channel is modeled as an independent Rayleigh fading channel, separately operating on each component. Perfect phase recovery and CSI are assumed at the receiver. We also assume that the system is unaffected by inter-symbol interference.

To satisfy the assumption of independence we need to introduce a component interleaver which destroys the correlation among the in-phase and quadrature channel fading coefficients. It should be evident that the component interleaving is the key point in obtaining any gain in the example of Figure 1. An undesirable effect of the component interleaver is the fact that it produces non constant envelope transmitted signals [8].

As a result of the above assumptions we will write the received vector as $\mathbf{r} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{n}$, where $\mathbf{n} = (n_1, n_2, \dots n_n)$ is a noise vector, whose real components n_i are zero mean, N_0 variance Gaussian distributed independent random variables, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots \alpha_n)$ are the

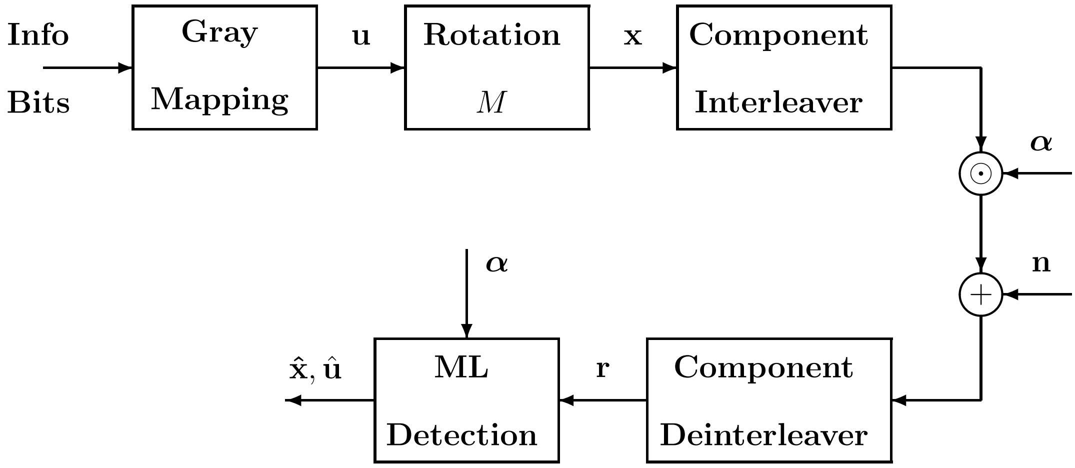

Fig. 2. System model

random fading coefficients with unit second moment and $\odot$ represents the component-wise product. Signal demodulation is assumed to be coherent, so that the fading coefficients can be modeled after phase elimination, as real random variables with a Rayleigh distribution and unit second moment ($E[\alpha_i^2] = 1$). The independence of the fading samples represents the situation where the components of the transmitted points are perfectly interleaved.

After de-interleaving the components of the received points, the maximum likelihood (ML) detection criterium with perfect CSI imposes the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \tag{1}$$

Using this criterium we obtain the decoded point $\hat{\mathbf{x}}$ and the corresponding integer component vector $\hat{\mathbf{u}}$ from which the decoded bits can be extracted.

The minimization of (1) can be a very complex operation for an arbitrary signal set with a large number of points. It is shown in [7] how to apply the *Universal lattice decoder* [6] to obtain a more efficient ML detection of lattice constellations in fading channels.

In [4], using the Chernoff bounding technique, we have shown that the point error probability of a multidimensional signal set is essentially dominated by four factors. To improve performance it is necessary to

1. Minimize the average energy per constellation point.
2. Maximize the diversity L.

3. Maximize the *minimum L-product distance*

$$d_{p,min}^{(L)} = \prod_{x_i \neq y_i}^{(L)} |x_i - y_i|$$

between any two points $\mathbf{x}$ and $\mathbf{y}$ in the constellation.

4. Minimize the *product kissing number* τ_p for the L-product distance i.e., the total number of points at the minimum L-product distance.

In this paper we have fixed the average energy of the constellations so we concentrate on the remaining items.

III. Algebraic number theory

The idea of rotating a two-dimensional QAM constellation was first presented in [10]. It was found that for a 16-QAM a rotation angle of $\pi/8$ gave a diversity of 2. The effect of this rotation is to spread the information contained in each component over both components of the constellation points. Pursuing a similar approach, the optimization of a four-dimensional rotation is found in [8]. The approach to determine such rotations is direct and can not be easily extended to multidimensional constellations.

A more sophisticated mathematical tool is needed to construct lattice multidimensional constellations with high diversity: *algebraic number theory.* A simple introduction to this theory is given in [4] together with a review of the known lattice constellations obtained from the canonical embedding of real and complex algebraic number fields.

Here we will briefly highlight some of the mathematical concepts in algebraic number theory, nevertheless we recommend some further readings on this topic [13], [14], [15].

An algebraic number field $K = \mathbf{Q}(\theta)$ is the set of all possible algebraic combinations $(+, -, *, /)$ of an algebraic number θ (real or complex, irrational and non transcendental) with the rational numbers of $\mathbf{Q}$. This set has all the field properties and is related to an irreducible polynomial over $\mathbf{Q}$, called the *minimal polynomial*, having θ as a root.

From elementary calculus we know that $\mathbf{Q}$ is *dense* in $\mathbf{R}$, the set of real numbers. Then we could state that the set K is 'a little bit denser' in $\mathbf{R}$ if K is a real field, and 'a little bit denser' in $\mathbf{C}$ if K is a complex field.[3] Using a particular mapping, called the *canonical embedding*, it is possible to uniquely represent each element of an algebraic number field with a point in an n-dimensional Euclidean space $\mathbf{R}^n$ just like we represent the elements of $\mathbf{Q}$ on the real line $\mathbf{R}$. This set of points is now only 'dense' in $\mathbf{R}^n$ as $\mathbf{Q}$ was 'dense' in $\mathbf{R}$. In fact we chose n so as to satisfy this condition. n is called the *degree* of the algebraic number field.

The parallel between $\mathbf{Q}$ and K can be further extended. In fact, within $\mathbf{Q}$ we find the set of relative integers $\mathbf{Z}$ which can be represented as a one dimensional lattice Z in $\mathbf{R}$. In K there exists a subset O_K, called the *ring of integers* or *integer ring* of K, which is mapped by the canonical embedding to an n-dimensional lattice, i.e. a discrete group of $\mathbf{R}^n$.

Finally, an *ideal* of $\mathbf{Z}$ can be viewed as a sub-lattice of Z, similarly an ideal of the ring of integers O_K is mapped by the canonical embedding into a sub-lattice of the lattice produced by O_K.

The interest in these lattices lies in the fact that they present a diversity which can be easily controlled by properly selecting the algebraic number field. A key result in [4] shows that it is possible to design lattice constellations with diversity ranging between $n/2$ and n according to the number of real (r_1) and complex ($2r_2$) roots of the minimal polynomial of the number field. In particular it is proven that $L = r_1 + r_2$. It is then shown that only for $L = n$, the $d_{p,min}$ is related to the particular field properties of K.

IV. Converting the Rayleigh fading channel into a Gaussian channel

In this section, we show that the multidimensional QAM constellation becomes insensitive to fading when the diversity L is large. This means that the point error probability is the same with or without fading. We focus the proof on the analysis of the pairwise point error probability $P(\mathbf{x} \to \mathbf{y})$, which is the probability of the received point $\mathbf{r}$ to be closer to $\mathbf{y}$ than to $\mathbf{x}$, assuming that $\mathbf{x}$ is transmitted. The detector selects $\mathbf{y}$ if $m(\mathbf{x}|\mathbf{r},\boldsymbol{\alpha}) \leq m(\mathbf{y},\mathbf{r},\boldsymbol{\alpha})$ and the conditional pairwise error probability is given by

$$P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = P(\sum_{i=1}^{n} |r_i - \alpha_i y_i|^2 \leq \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2) = P(X \geq A)$$

[3]We note that this intuitive idea is mathematically unprecise since K has the same density of $\mathbf{Q}$ in $\mathbf{R}$.

where $X = \sum_{i=1}^{n} \alpha_i (x_i - y_i) n_i$ is a Gaussian random variable and $A = \frac{1}{2} \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2$ is a constant. The mean of X is zero and its variance is $\sigma_X^2 = 2N_0 A$. The conditional pairwise error probability can be written as $P(\mathbf{x} \to \mathbf{y} | \boldsymbol{\alpha}) = Q(A/\sigma_X)$ and we obtain

$$P(\mathbf{x} \to \mathbf{y} | \boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2}{4N_0}}\right) \tag{2}$$

We recall that the Gaussian tail function is defined as $Q(x) = (2\pi)^{-1/2} \int_x^\infty \exp(-t^2/2) dt$. The pairwise error probability $P(\mathbf{x} \to \mathbf{y})$ is obtained by averaging over the fadings α_i,

$$P(\mathbf{x} \to \mathbf{y}) = \int P(\mathbf{x} \to \mathbf{y} | \boldsymbol{\alpha}) f(\boldsymbol{\alpha}) d\boldsymbol{\alpha}$$

where $f(\boldsymbol{\alpha})$ is the probability density function (p.d.f.) of the fading coefficients. The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is at least L, since L is the modulation diversity of the constellation. For simplicity of notations and without loss of generality, we assume that $|x_i - y_i| = 1$ for the first L components and $|x_i - y_i| = 0$ for the other $n - L$ components. The conditional pairwise error probability given by (2) becomes

$$P(\mathbf{x} \to \mathbf{y} | \boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{\sum_{i=1}^{L} \alpha_i^2}{4N_0}}\right) . \tag{3}$$

On a Gaussian channel, expression (3) simplifies to

$$P(\mathbf{x} \to \mathbf{y}) = Q\left(\sqrt{\frac{L}{4N_0}}\right) = Q\left(\frac{d_E(\mathbf{x}, \mathbf{y})}{2\sigma}\right) \tag{4}$$

where $d_E^2(\mathbf{x}, \mathbf{y}) = L$ is the squared Euclidean distance between $\mathbf{x}$ and $\mathbf{y}$ and $\sigma^2 = N_0$ is the noise variance.

At first sight, one can say that $\sum_{i=1}^{L} \alpha_i^2$ acts as $E[\sum_{i=1}^{L} \alpha_i^2] = L$ when L goes to infinity. This is the *weak law of large numbers*. It states that $\sum_{i=1}^{L} \alpha_i^2 / L$ converges to 1 since the variance of the sum tends to zero. The probability that the difference is larger than a threshold in absolute value is small. The convergence is very weak and can be proved using the Chebychev inequality. It shows, roughly and intuitively, that (3) approaches (4) and thus the fading has no effect when L is very large.

The above discussion does not constitute a rigorous proof. The exact proof is found when applying the *strong law of large numbers* (convergence in the sense of probability laws), as done below.

First, let us rewrite the conditional pairwise error probability as

$$P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{L(1+Y)}{4N_0}}\right) \tag{5}$$

where $Y = \frac{\sum_{i=1}^{L}(\alpha_i^2-1)}{L} = \sum_{i=1}^{L} Y_i$. The random variables $Y_i = (\alpha_i^2 - 1)/L$ have a central χ^2 distribution [12] with 2 degrees of freedom, because $\alpha_i^2 = a_i^2 + b_i^2$ where a_i and b_i are two statistically independent and identically distributed Gaussian variables with zero mean and variance 1/2. The mean and the variance of Y_i are respectively $E[Y_i] = 0$ and $E[Y_i^2] = 1/L^2$. As a consequence of the statistical independence of the Y_i, their sum Y is a χ^2 random variable with $2L$ degrees of freedom. Its mean and variance are respectively $E[Y] = 0$ and $E[Y^2] = 1/L$. The p.d.f. of Y is given by

$$f_Y(y) = \frac{L^L}{(L-1)!}(y+1)^{L-1}\exp(-L(y+1)), \qquad y \geq -1 \tag{6}$$

Figure 3 shows the p.d.f. for $L = 2, 4, 8, 12, 16$ and 32. Clearly, we see that $f_Y(y)$ tends to a Dirac impulse $\delta(y)$ when L goes to infinity. More precisely, it is easy to show that $\int_{-\infty}^{\infty} f_Y(y)g(y)dy \rightarrow g(0)$ when $L \rightarrow \infty$, for any function g of the class $C^\infty(-\infty, \infty)$. From the definition of the Dirac distribution we can say that $f_Y(y) \rightarrow \delta(y)$. Hence, the pairwise error probability

$$P(\mathbf{x} \rightarrow \mathbf{y}) = \int \mathrm{Q}\left(\sqrt{\frac{L(1+Y)}{4N_0}}\right) f_Y(y)dy$$

approaches the pairwise error probability of the Gaussian channel $Q(\sqrt{\frac{L}{4N_0}})$.

An exact expression of $P(\mathbf{x} \rightarrow \mathbf{y})$ can also be obtained by combining expressions (5) and (6). and directly computing the above integral. This yields $P(\mathbf{x} \rightarrow \mathbf{y})$ as a function of the signal-to-noise ratio $SNR = L/N_0$,

$$P(\mathbf{x} \rightarrow \mathbf{y}) = \left(\frac{1-\mu}{2}\right)^L \times \sum_{k=0}^{L-1} \left(\begin{array}{c} L+k-1 \\ k \end{array}\right) \left(\frac{1+\mu}{2}\right)^k \tag{7}$$

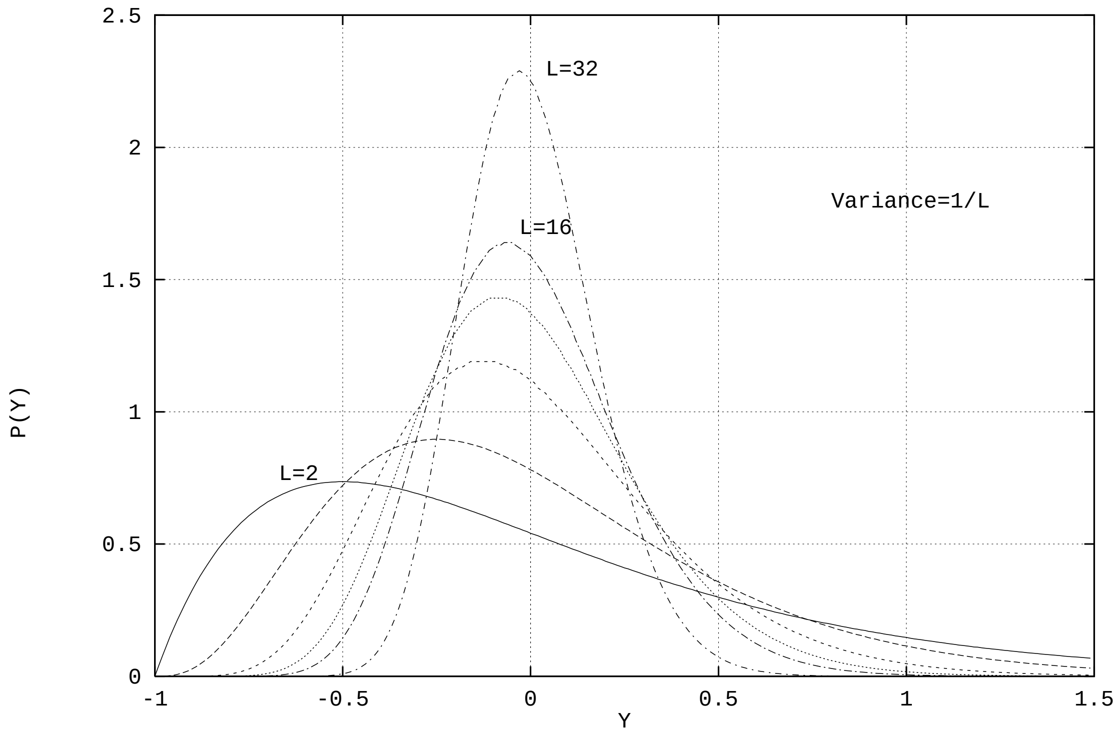

Fig. 3. Probability density function of Y

where μ is given by

$$\mu = \sqrt{\frac{\frac{SNR}{8L}}{1 + \frac{SNR}{8L}}}$$

The pairwise error probability of (7) is plotted in Figure 4 for diversities $L = 1$, 4, 12 and 32 on the Rayleigh fading channel. We also plotted in Figure 4 the pairwise error probability of (4) on the additive white Gaussian noise channel (AWGN). Practically, the fading effect is reduced when diversity is larger or equal to 12, as shown by Figure 4 and confirmed by the simulation results in Section VII.

V. Rotating the integer lattice Z^n

This section collects the three techniques we have investigated to obtain a rotated multi-dimensional cubic lattice Z^n with high diversity. Following the notations of [4] we denote with $\Lambda_{n,L}$ an n-dimensional lattice with diversity L.

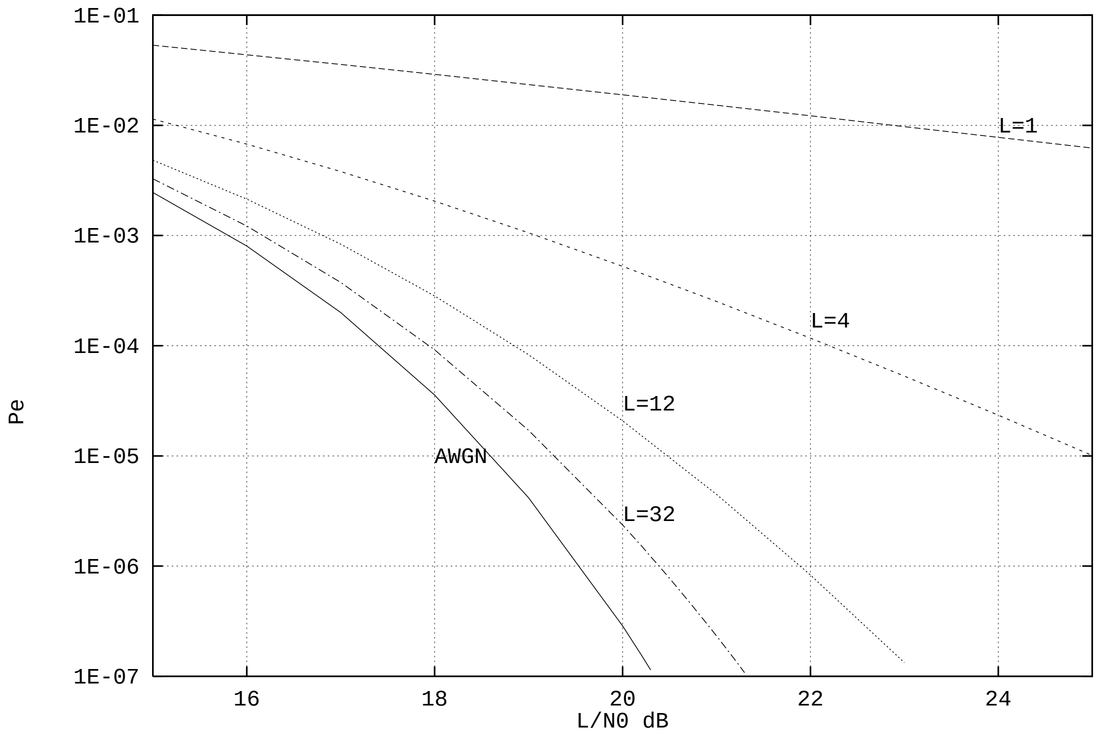

Fig. 4. Pairwise error probability

We observe that the generator matrix M of the rotated lattice Z^n is actually a rotation matrix which transforms all the integer component vectors into a set of vectors with the required diversity.

The rotated cubic lattice constellation can be either used as an uncoded multidimensional modulation scheme or as a base modulation for further coding techniques. For example, we could apply these rotations to any known coding scheme based on QAM modulations to obtain the benefits of diversity together with the coding gain.

A. Construction of rotated Z^n lattices from known rotated integral lattices

In [4] the rotated versions of the lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ are found for L equal to half the dimension. Since $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ are integral lattices (i.e., sub-lattices of Z^n) we expected to find the under-laying rotated Z^n lattice with the same diversity. In this section we will briefly discuss this problem.

We say that two lattices Λ_1 and Λ_2 are *equivalent* if they are equal up to a rotation and a scaling factor. The generator matrices M_1 and M_2 of two equivalent lattices are related by

$$M_2 = \alpha B M_1 R \tag{8}$$

where α is the scaling factor, R is the rotation matrix ($\det(R) = \pm 1$) and B is a lattice basis transformation matrix i.e., an integer matrix with $\det(B) = \pm 1$. The matrix B is also known as an integer unimodular matrix.

Let us denote any one of the non rotated lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ with $\Lambda_{n,1}$ since it has diversity $L = 1$ and with $\Lambda_{n,n/2}$ the corresponding rotated lattice with diversity $L = n/2$. The two lattices $\Lambda_{n,1}$ and $\Lambda_{n,n/2}$, defined by the generator matrices M_1 and M_2, are equivalent. If we determine the scaling factor α and the matrix B then we are able to obtain the desired rotation matrix R from (8).

Taking the absolute value of the determinant of both sides of (8) we obtain

$$\alpha = \left(\frac{|\det M_2|}{|\det M_1|} \right)^{1/n} .$$

Without loss of generality we can replace M_2 by $\alpha^{-1} M_2$ and concentrate on finding B. Let us consider the Gram matrices $G_1 = M_1 M_1^T$ and $G_2 = M_2 M_2^T$. Since $M_2 = R M_1 B$ we have $G_2 = B G_1 B^T$. Instead of finding B we search directly for a generator matrix M_1 of the non rotated lattice which results in $G_2 = G_1 = M_1 M_1^T$, implying that B is the identity matrix.

The Gram matrix G_2 is symmetric and its elements g_{ij} are the scalar products $\langle \mathbf{v_i}, \mathbf{v_j} \rangle$ of the lattice basis vectors corresponding to the rows of M_1. The diagonal elements g_{ii} correspond to the square norms of the basis vectors. The problem is then to determine the generator matrix M_1 such that the lattice basis vectors satisfy the conditions on the scalar products imposed by G_2. By computer search we were able to find the generator matrices M_1 and the desired rotation matrices $R = M_2 M_1^{-1}$.

B. Algebraic construction of $Z_{n,n/2}$ lattices

In this section we construct a family of orthogonal matrices with diversity $L = n/2$ for $n = 2^{e_1} 3^{e_2}$, $e_1, e_2 = 0, 1, 2, \ldots$ applying the canonical embedding to some totally complex cyclotomic number fields. For the mathematical details about algebraic number fields and the canonical embedding the reader can refer to [4].

The key points used in this section to find $Z_{n,n/2}$ are the following :

- The vectors of the lattice basis are orthogonal.
- The minimal polynomial $\mu_\theta(x)$ has integer coefficients.
- The minimal polynomial $\mu_\theta(x)$ has n distinct complex roots.
- The lattice dimension is $n = \Phi(N)/2$, where $\Phi(\cdot)$ is the Euler function giving the number of integers prime with N [14].

Let us consider the cyclotomic field $K = \mathbf{Q}[j](\theta)$, where $\theta = e^{2\pi j/N}$ is an N-th root of unity. K is an algebraic extension of $\mathbf{Q}[j] = \{a + jb | a, b \in \mathbf{Q}\}$ of degree $\Phi(N)/2$. We recall that this is a totally complex field with signature $(r_1 = 0, r_2 = n/2)$ and minimal polynomial

$$\mu_\theta(x) = \prod_{(k,N)=1} (x - \theta^k) \tag{9}$$

where (k, N) is the greatest common divisor of k and N. The minimal polynomial over $\mathbf{Z}[j]$ is denoted by $m(x)$ and defined later in this section.

Let us denote $\theta_1 = \theta, \theta_2, \ldots \theta_{n/2}$ the complex roots of $\mu_\theta(x)$ which define the $n/2$ distinct field $\mathbf{Q}$-homomorphisms

$$\sigma_1(\theta) = \theta_1,\ \sigma_2(\theta) = \theta_2,\ \ldots\ \sigma_{n/2}(\theta) = \theta_{n/2}\ . \tag{10}$$

To construct a complex lattice Λ of dimension $n/2$ we apply the canonical embedding to the ring of integers $O_K = \mathbf{Z}[j](\theta)$ generated by $(1, \theta, \theta^2, \ldots \theta^{n/2-1})$. Its generator matrix is given by

$$M = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_{n/2} \\ \vdots & \vdots & & \vdots \\ \theta_1^{n/2-1} & \theta_2^{n/2-1} & \ldots & \theta_{n/2}^{n/2-1} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_{n/2} \end{pmatrix} \tag{11}$$

where the complex lattice basis vectors $\mathbf{v}_i$, $i = 1, 2, \ldots n/2$, correspond to the rows of M.

The corresponding real lattice of dimension n can be obtained by replacing each complex entry $a + jb$ of M by a 2×2 matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. As proven in [4] this lattice has diversity $L = n/2 = r_2$.

We are interested in selecting the roots θ_i, $i = 1, 2, \dots n/2$, or equivalently their minimal polynomial $\mu_\theta(x)$, so that M becomes an orthogonal matrix i.e., a generator matrix for the complex integer lattice in dimension $n/2$. The orthogonality among the complex vectors implies the orthogonality among the corresponding real vectors. The complex inner product of any two rows $\mathbf{v}_{p+1} = (\theta_1^p, \theta_2^p, \dots \theta_{n/2}^p)$ and $\mathbf{v}_{q+1} = (\theta_1^q, \theta_2^q, \dots \theta_{n/2}^q)$, $p, q = 0, 1, \dots n/2 - 1$ of M must satisfy

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k)^p (\theta_k^*)^q = \begin{cases} 1 & p = q \\ 0 & p \neq q \end{cases} \tag{12}$$

For $p > q$, we have

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k \theta_k^*)^q (\theta_k)^{p-q} = \sum_{k=1}^{n/2} \|\theta_k\|^q (\theta_k)^{p-q} = 0 \tag{13}$$

and since the complex roots θ_i are placed on the unit circle $\|\theta_k\| = 1$

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k)^m = S_m = 0 \qquad m = 1, 2, , \dots n/2 - 1 \tag{14}$$

In other words, the first $n/2 - 1$ power symmetric functions S_m of the roots of $\mu_\theta(x)$ are null. The polynomial $\mu_\theta(x)$, which we want to determine, can be factored into $m(x)m^*(x)$, where we assume that θ_i, $i = 1, 2, \dots n/2$ are the roots of the polynomial $m(x)$ of degree $n/2$ over the ring of Gaussian integers $\mathbf{Z}[j]$, while $m^*(x)$ takes on the complex conjugate roots.

Applying Newton's identities one easily observes that $m(x) = (x - \theta_1) \cdots (x - \theta_{n/2}) = x^{n/2} + P$ and $m^*(x) = x^{n/2} + P^*$ so that

$$\mu_\theta(x) = x^n + (P + P^*) x^{n/2} + 1 \ . \tag{15}$$

Now that we have the general form of the minimal polynomial we still need to determine which of the n roots of unity must be chosen to apply the canonical embedding (11).

Let $\theta_i = e^{j\phi_i}, i = 1, 2, \ldots n/2$ be the unknown roots of $m(x)$ which we want to determine. P is the product of the $n/2$ roots laying on the unit circle

$$P = e^{j\psi} \qquad -\pi \leq \psi < \pi \tag{16}$$

thus

$$m(\theta_i) = e^{j\phi_i n/2} + e^{j\psi} = 0 \tag{17}$$

and we obtain exactly $n/2$ distinct values of θ_i with

$$\phi_i = 2\frac{\psi + \pi}{n} + \frac{4\pi(i-1)}{n} \qquad i = 1, 2, \ldots n/2 \tag{18}$$

Similarly, for the roots $\theta_{i+n/2} = e^{j\phi_{i+n/2}}$ of $m^*(x)$ satisfy

$$\phi_{i+n/2} = 2\frac{\pi - \psi}{n} + \frac{4\pi(i-1)}{n} \qquad i = 1, 2, \ldots n/2 \tag{19}$$

In order to determine the value of ψ we consider the following conditions

- $\mu_\theta(x)$ has exactly n distinct roots, so the roots of $m(x)$ must be different from the roots of $m^*(x)$

$$2\frac{\pi + \psi}{n} \neq 2\frac{\pi - \psi}{n} \quad \Rightarrow \quad \psi \neq 0 \tag{20}$$

- $\mu_\theta(x)$ has only complex roots, so

$$\phi_i, \phi_{i+n/2} \neq k\pi \quad \Rightarrow \quad 2\pi i + \pi \pm \psi \neq \frac{n}{2}k\pi \quad \Rightarrow \quad \psi \neq 0 \tag{21}$$

- $\mu_\theta(x)$ has integer coefficients

$$P + P^* = e^{j\psi} + e^{-j\psi} = 2\cos\psi \in \mathbf{Z} \tag{22}$$

  which implies $\psi = \pm\pi/3, \pm\pi/2, \pm 2\pi/3$.

The possible values for the roots of $m(x)$ are summarized in Table I, where only the negative values of ψ were considered since the positive ones correspond to the roots of $m^*(x)$. The third column (the value of N) is derived from the second one by noting that $\phi_1 = 2\pi/N$ since by definition $\theta = e^{2\pi j/N} = \theta_1 = e^{j\phi_1}$.

ψ	$\phi_i = 2\frac{\psi+\pi}{n} + \frac{4\pi(i-1)}{n}$	N
$-\frac{\pi}{3}$	$\frac{4\pi}{3n} + \frac{4\pi(i-1)}{n}$	$\frac{3n}{2}$
$-\frac{\pi}{2}$	$\frac{\pi}{n} + \frac{4\pi(i-1)}{n}$	$2n$
$-\frac{2\pi}{3}$	$\frac{2\pi}{3n} + \frac{4\pi(i-1)}{n}$	$3n$

TABLE I

THE ADMISSIBLE VALUES FOR THE ROOTS ARE $\theta_i = e^{j\phi_i},\ i = 1, \ldots n/2$

Finally, we must solve $\Phi(N) = n$ for $N = 3n/2, 2n, 3n$, to obtain the admissible values of the dimension n of the real lattice. Equivalently we can solve $\Phi(N)/N = 1/K$ where $N = Kn$ for $K = 2, 3, 3/2$. We recall that $\Phi(N)/N$ must have the largest prime dividing N as a factor in the denominator. Then for the above Ks the largest prime in N is at most 3 and we can write $N = 2^{e_1}3^{e_2}$ for some $e_1, e_2 = 0, 1, 2, \ldots$. We distinguish the three cases:

$\mathbf{N = 3n/2}$ — Let $N = 2^{e_1}3^{e_2}$ with $e_1 = 0, 1, 2, \ldots$, $e_2 = 1, 2, \ldots$, then $\Phi(3n/2) = n$ has no solutions.

$\mathbf{N = 2n}$ — In this case the largest prime dividing N is at most 2, so that $N = 2^{e_1}$ with $e_1 = 1, 2, \ldots$, then $\Phi(2n) = n$ has solutions for $n = 2^{e_1}$.

$\mathbf{N = 3n}$ — Let $N = 2^{e_1}3^{e_2}$ with $e_1 = 0, 1, 2, \ldots$, $e_2 = 1, 2, \ldots$, then $\Phi(3n) = n$ has solutions for $n = 2^{e_1}3^{e_2}$.

We can conclude that the admissible values of ψ are $-\pi/2$ and $-2\pi/3$. They correspond to the polynomials of the type $x^n + \epsilon x^{n/2} + 1$ with $\epsilon = 0$ or -1 and with $N = 2n$ and $3n$ respectively. Thus, there exist $Z_{n,n/2}$ lattices for all dimensions $n = 2^{e_1}3^{e_2}$, with $e_1 = 1, 2, \ldots$ and $e_2 = 0, 1, 2, \ldots$.

C. Algebraic construction of $Z_{n,n}$ lattices

This construction is based on the totally real algebraic number field $\mathbf{Q}(2\cos(2\pi/N))$. By applying the canonical embedding to a particular ideal in this field we found the rotated cubic lattice $Z_{n,n}$. Since $\mathbf{Q}(2\cos(2\pi/N))$ is a totally real field we know from [4] that the constellation has full diversity $L = n$. The choice of this family of number fields appears to be arbitrary but in the following section we will show that some of these rotated cubic lattices also maximize the product distance of the constellation.

We now describe the procedure we used to obtain $Z_{n,n}$. We know that the degree of $\mathbf{Q}(2\cos(2\pi/N))$ is $\Phi(N)/2$. This imposes some limitations on the lattice dimensions we can obtain ($n = \Phi(N)/2$). All the even dimensions up to 32 do not lead to the desired integer lattice while the odd ones in Table II do. The procedure is the following:

1. Consider the number field $K = \mathbf{Q}(2\cos(2\pi/N))$ with minimal polynomial $\mu_\theta(x)$ (see Appendix A) and absolute discriminant d_K.
2. Let $d_K = p^m$ be the prime factorization of the absolute discriminant.
3. Factor the principal ideal (p) into I^n, where I is a prime ideal.
4. For $k = 0, \dots n$ apply the canonical embedding to the ideal I^k and check if the generator matrix is orthogonal i.e., the generator matrix of $Z_{n,n}$.

The last column of Table II gives the power of the ideal I which produces the full diversity $Z_{n,n}$ lattice. The lattice is given by $Z_{n,n} = \sigma(I^k)$, where σ is the canonical embedding defined by the n real roots of $\mu_\theta(x)$. The fundamental volume of $Z_{n,n}$ can be related to d_K and the algebraic norm $N(I^k) = p^k$ by [4]

$$vol(Z_{n,n}) = N(I^k) * \sqrt{|d_K|}\ .$$

If we introduce a scaling factor $\alpha = (p^k * \sqrt{|d_K|})^{1/n}$, we obtain the unit volume cubic lattice.

As an example, the full diversity cubic lattice $Z_{5,5}$ is found from the field $\mathbf{Q}(2\cos(2\pi/11))$. The absolute discriminant is $d_K = 11^4$ and $Z_{5,5} = \sigma(I^3)$. The prime ideal I is computed by factoring the principal ideal generated by 11: $(11) = (11, \theta + 2)^5$ and $I = 11O_K + (\theta + 2)O_K$.

VI. Maximizing the product distance

In the previous section we have shown how to obtain rotated Z^n lattices which guarantee a certain degree of diversity. Although diversity appears to be the most relevant design parameter we are also interested in maximizing the minimal product distance $d_{P,min}$ between

n	N	$\mu_\theta(x)$	d_K	k
3	$7, 14$	$x^3 + x^2 - 2x - 1$	7^2	2
	$9, 18$	$x^3 - 3x + 1$	3^4	1
5	$11, 22$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11^4	3
9	$19, 38$	$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5$ $+15x^4 - 20x^3 - 10x^2 + 5x + 1$	19^8	5
11	$23, 46$	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6$ $-56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	23^{10}	6
15	$31, 62$	$x^{15} + x^{14} - 14x^{13} - 13x^{12} + 78x^{11} + 66x^{10} -$ $220x^9 - 165x^8 + 330x^7 + 210x^6 - 252x^5 -$ $126x^4 + 84x^3 + 28x^2 - 8x - 1$	31^{14}	8

TABLE II

FULL DIVERSITY $Z_{n,n}$ LATTICES FROM IDEALS OF THE $\mathbf{Q}(2\cos(2\pi/N))$.

any two points of the constellation. In this section we show a construction of $Z_{n,n}$ lattices for some even n which aims at maximizing $d_{P,min}$.

Stating the problem in the the most general form, we need to determine an arbitrary rotation matrix, with the highest possible diversity order ($L = n$), which maximizes $d_{P,min}$ of the corresponding signal constellation. This optimization problem becomes rapidly intractable due to the number of variables and the complexity of the constraints. For this reason we restrict our search to a smaller family of rotation matrices which can be parameterized with a reduced number of variables and result in simpler constraints.

We start with dimensions 2 and 3 and then move up to other dimensions of the type $2^{e_1}3^{e_2}$ applying a construction which recalls the one used for Hadamard matrices.

It is important to remind that whenever we are dealing with lattices generated by canonical embedding of totally real number fields $d_{P,min}$ is related to the field norm and is independent of the size of the finite constellation carved from the lattice [4]. In all other cases this is not

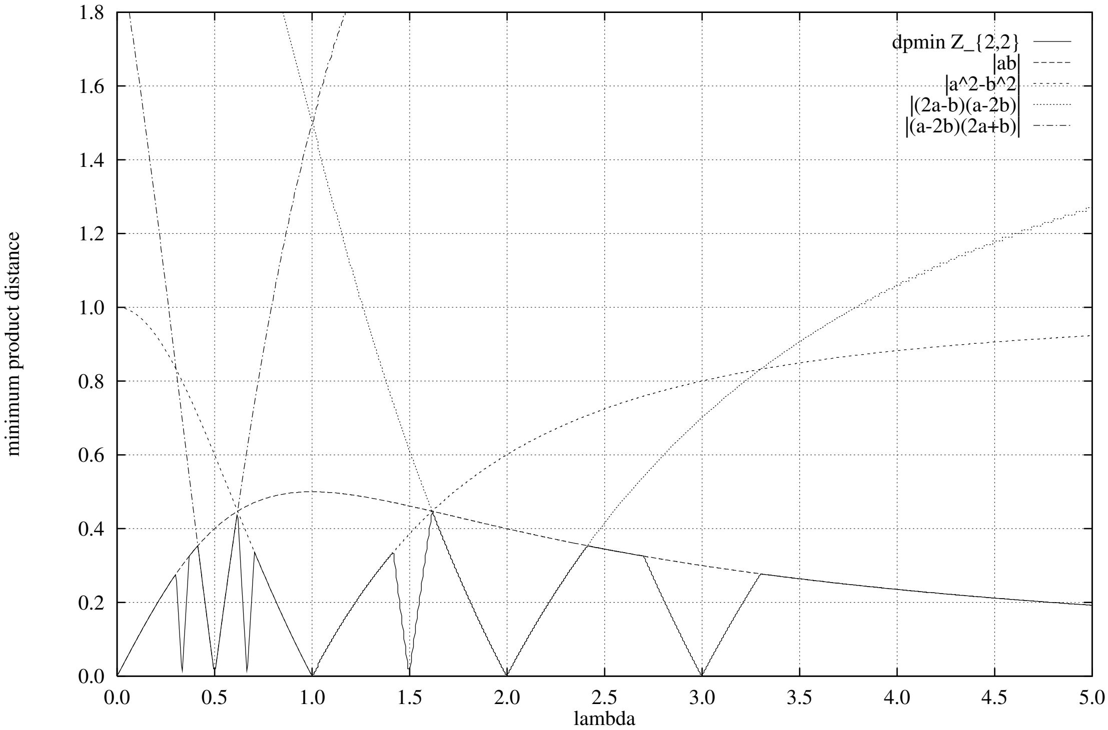

Fig. 5. $d_{P,min}$ for a family of $Z_{2,2}$ lattices

necessarily true.

In the following $d_{P,min}$-optimizing construction we limited the size of the constellations to the case of $\eta = 4$ bits/symbol. In all cases (except for the three-dimensional one, where it is proven to be true) we verified experimentally that $d_{P,min}$ does not depend on the size of the constellation. We conjecture that in all these cases we are dealing with some lower dimensional sections of a lattice generated by canonical embedding of totally real number fields of higher degree.

A. Dimension 2

All two-dimensional orthogonal matrices have the following structure

$$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

with the constraint $a^2 + b^2 = 1$.

We parameterize this orthogonal matrix as a function of the single variable λ as follows

$$a = 1/\sqrt{1+\lambda^2} \qquad b = \lambda a \ .$$

Note that the rows of M are the normalized orthogonal lattice basis vectors. Figure 5 shows the values of $d_{P,min}$ as a function of λ for a finite constellation ($\eta = 4$ bits/symbol), carved from the lattice generated by M. Only positive values of λ were considered due to the symmetry about the origin and the values of λ resulting in $L = 1$ diversity constellation were skipped. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation using a small step for λ (e.g. 0.005). In the same figure we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b| & (1,0) \\ |a^2 - b^2| & (1,1) \\ |(2a-b)(a+2b)| & (2,1) \\ |(a-2b)(2a+b)| & (1,2) \end{cases} \tag{23}$$

corresponding to the product distances between the origin and the points with the integer components reported in the second column of (23). The curve of $d_{P,min}$ could, in principle, be obtained as the minimum of all the bounds of the type (23) for all the points of the constellation.

In Figure 5 we observe that the highest peaks are found at the intersection of the first and second bound in (23) that is for

$$\lambda_{o,2} = \frac{1 \pm \sqrt{5}}{2} \qquad d^{o,2}_{P,min} = \frac{\sqrt{5}}{5} < 0.5 \ . \tag{24}$$

The upper bound of 0.5 to $d_{P,min}$ is obtained by assuming that there exists a constellation containing a unit norm vector with all equal components.

A few considerations about the optimal matrix are appropriate here. $\lambda_{o,2}$ is the root of the polynomial $\lambda^2 + \lambda - 1$ i.e., it belongs to a totally real number field of degree 2. The entries a and b of M then belong to a number field of degree 4. In this case we are not using the canonical embedding lattice but probably some two-dimensional section of it, which gives us a Z^2 lattice constellation with diversity $L = 2$ and maximal $d_{P,min}$. The two dimensional case is the only one where we have obtained the absolute maximum $d_{P,min}$ among all possible rotation matrices.

B. Dimension 3

The family of three-dimensional orthogonal matrices we consider here is

$$M = \begin{pmatrix} a & b & c \\ b & c & a \\ -c & -a & -b \end{pmatrix}$$

with the constraints $a^2 + b^2 + c^2 = 1$ and $ab + bc + ac = 0$.

We parameterize this orthogonal matrix as a function of the single variable λ as follows

$$a = \frac{1+\lambda}{1+\lambda+\lambda^2} \qquad b = \lambda a \qquad c = \frac{-\lambda}{1+\lambda} a \ . \tag{25}$$

As before the rows of M form the orthonormal lattice basis vectors of a rotated version of Z^3.

Figure 6 shows the values of $d_{P,min}$ as a function of λ, for a finite constellation with $\eta = 4$ bits/symbol, carved from the lattice generated by M. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation for each value of λ. In this case the values of λ were taken in the range $(-4, 4)$ since the $d_{P,min}$ rapidly vanishes outside this interval. The values of λ resulting in diversity less than 3 were skipped. In Figure 6 we also plot the following upper bounds to $d_{P,min}$

$$d_{P,min} \leq \begin{cases} |a\,b\,c| & (1,0,0) \\ |(a-b)(b-c)(c-a)| & (1,0,1) \\ |(a+b-c)(b+c-a)(c+a-b)| & (1,1,1) \end{cases} \tag{26}$$

corresponding to the product distances between the origin and the points with the integer components reported in the second column of (26).

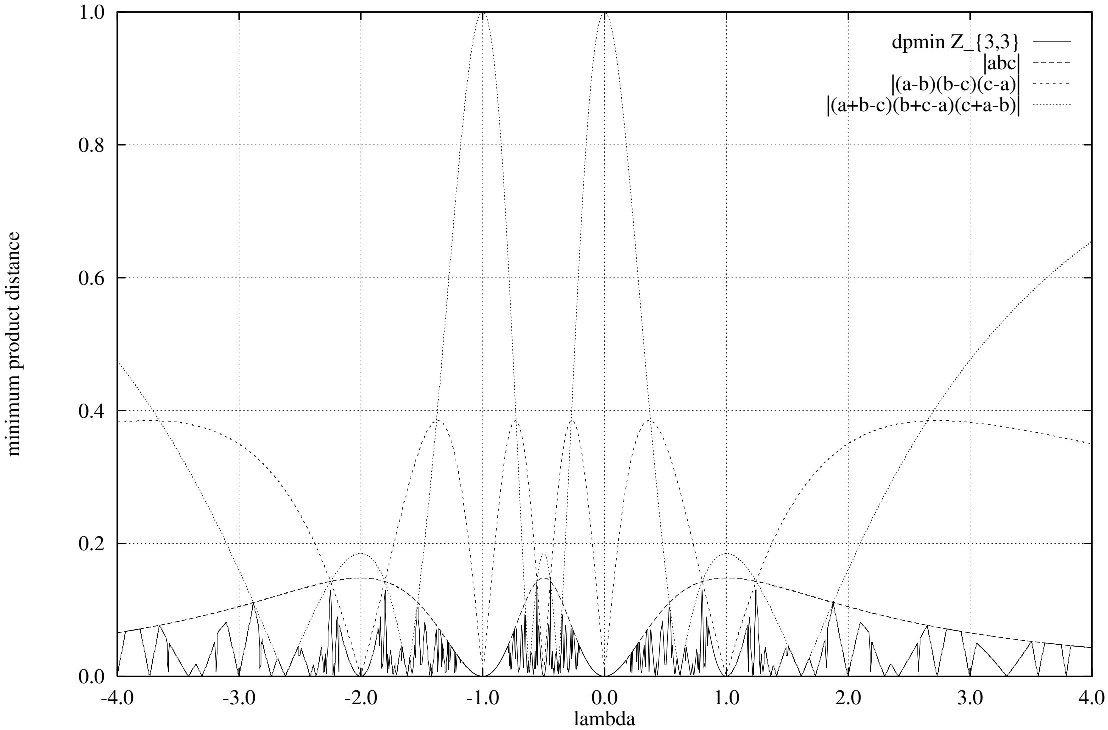

Fig. 6. $d_{P,min}$ for a family of $Z_{3,3}$ lattices

In Figure 6, we identify the highest peaks at the intersection of the first and second bound in (26), that is at the roots of the polynomials

$$\begin{aligned} p_1(\lambda) &= \lambda^3 + 2\lambda^2 - \lambda - 1 \\ p_2(\lambda) &= \lambda^3 + \lambda^2 - 2\lambda - 1 \ . \end{aligned}$$

Surprisingly, these two polynomials happen to be equivalent minimal polynomials of the totally real algebraic number field $\mathbf{Q}(2\cos(2\pi/7))$. The values $\lambda_{o,3}$ of the roots of the above polynomials have the simple expressions:

$$\begin{aligned} p_1 &: \ [2\cos(4\pi/7)]^{-1} = -2.24698, \quad [2\cos(6\pi/7)]^{-1} = -0.55496, \quad [2\cos(2\pi/7)]^{-1} = 0.80194 \\ p_2 &: \ 2\cos(6\pi/7) = -1.80194, \quad 2\cos(4\pi/7) = -0.44504, \quad 2\cos(2\pi/7) = 1.24698 \ . \end{aligned}$$

The values of $a(\lambda_{o,3}), b(\lambda_{o,3})$ and $c(\lambda_{o,3})$ to replace in M can be either computed directly by substitution in equations (25) or by applying the field properties of $\mathbf{Q}(2\cos(2\pi/7))$. This second method is preferable since it results in simple polynomial expressions:

$$
\begin{aligned}
a(\lambda_{o,3}) &= \left[\frac{1+\lambda}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(5+\lambda_{o,3}-\lambda_{o,3}^2) \\
b(\lambda_{o,3}) &= \left[\frac{\lambda+\lambda^2}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(-1+4\lambda_{o,3}+3\lambda_{o,3}^2) \\
c(\lambda_{o,3}) &= \left[\frac{-\lambda}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(3-5\lambda_{o,3}-2\lambda_{o,3}^2) \qquad (i=1,2)\ .
\end{aligned}
$$

Similarly, we can compute the optimal value $d_{P,min}^{o,3}$:

$$
d_{P,min}^{o,3} = [|a\,b\,c| \bmod p_i(\lambda)]_{\lambda=\lambda_{o,3}} = \left[\frac{\lambda^2(1+\lambda)^2}{(1+\lambda+\lambda^2)^3} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7} < \frac{1}{3} \quad (i=1,2)
$$

By direct inspection we find that all these lattices are equivalent to the lattices $Z_{3,3a}$ and $Z_{3,3b}$ of Section 3.3.

C. Construction in higher dimensions

In the two previous subsections we have found the basic building blocks of the rotation matrices we will present here. This construction is based on the special structure of some orthogonal matrices similar to the one used to construct Hadamard matrices. We will illustrate this construction in some detail for dimension 4. The other rotation matrices for dimensions 6, 8 and 12 are obtained by iterating the same construction.

C.1 Dimension 4

The family of four-dimensional orthogonal matrices we consider here is

$$
M = \begin{pmatrix} a & b & -c & -d \\ -b & a & d & -c \\ c & d & a & b \\ -d & c & -b & a \end{pmatrix} = \begin{pmatrix} M_1 & -M_2 \\ M_2 & M_1 \end{pmatrix}
$$

Let $U^2 = a^2+b^2+c^2+d^2$ be the normalization factor.

If the 2×2 sub-matrix M_1 is fixed to be one of the optimal two-dimensional matrices, then the orthogonality constraints reduce to $ad-bc=0$. The other 2×2 sub-matrix M_2 is

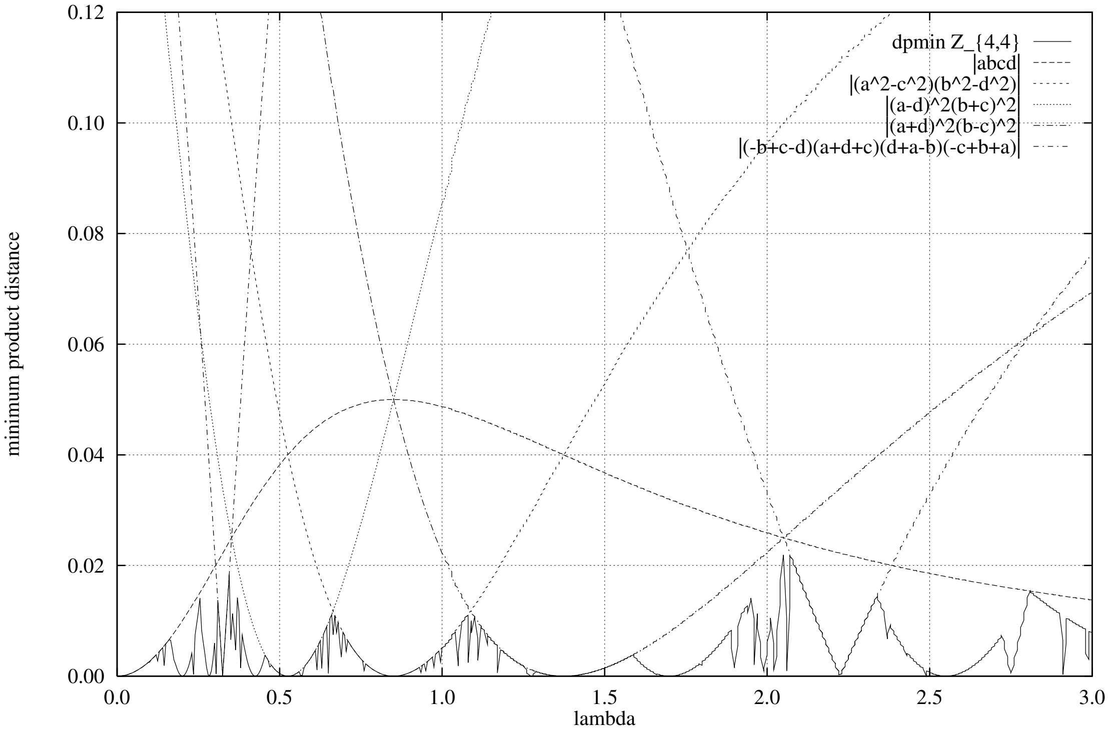

Fig. 7. $d_{P,min}$ for a family of $Z_{4,4}$ lattices

dependent on the parameter λ. The basis vectors are finally normalized by U giving

$$a = \frac{1}{U\sqrt{1+\lambda_{o,2}^2}} \qquad b = \frac{\lambda_{o,2}}{U\sqrt{1+\lambda_{o,2}^2}} \qquad c = \frac{\lambda}{U\lambda_{o,2}} \qquad d = \frac{\lambda}{U}$$

where

$$U = \frac{\sqrt{\lambda_{o,2}^2 + \lambda^2 + \lambda_{o,2}^2\lambda^2}}{\lambda_{o,2}} \,.$$

Figure 7 shows the values of $d_{P,min}$ as a function of λ for a finite constellation ($\eta = 4$ bits/symbol), carved from the lattice generated by M. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation. The values of λ are shown, with steps of 0.005, in the range $(0, 3)$, since the $d_{P,min}$ rapidly vanishes outside this interval and the curve is symmetric about the origin. The values of λ resulting in diversity less than 4 were skipped. In Figure 7 we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b\,c\,d| & (1,0,0,0) \\ |(a^2-c^2)(b^2-d^2)| & (1,0,1,0) \\ |(a-d)^2(b+c)^2| & (1,0,0,1) \\ |(a+d)^2(b-c)^2| & (0,1,1,0) \\ |(-b+c-d)(a+d+c)(d+a-b)(-c+b+a)| & (0,1,1,1) \end{cases} \tag{27}$$

corresponding to the product distances between the origin and the points with the given integer components.

In Figure 7 we find identify the two highest peaks at the intersection of the first and third bound in (27)

$$\lambda_{o,4}^{(1)} = \frac{1}{10}(\sqrt{2}-1)\sqrt{50+10\sqrt{2}} = 0.3523511$$

and at the intersection of the first and fourth bound in (27)

$$\lambda_{o,4}^{(2)} = \frac{1}{10}(\sqrt{2}+1)\sqrt{50+10\sqrt{2}} = 2.0536527\ .$$

These values can be obtained in a closed form since they are roots of a polynomial of degree 4. The corresponding optimal value for $d_{P,min}$ is $1/40$. Other two lower peaks are found at the intersection of the second and third bound in (27) ($\lambda_{so,4}^{(1)} = 0.6641681$) and at the intersection of the second and fourth bound in (27) ($\lambda_{so,4}^{(4)} = 1.0894935$). The corresponding sub-optimal value for $d_{P,min}$ is $1/85$. Closed form values of λ_{so}, can also be found.

C.2 Dimension 6

By a similar procedure we can build the six-dimensional orthogonal matrices starting from the optimal three-dimensional one. This is the highest dimension where closed-form solutions can be computed and we find one optimal value $1/(7^2\,5\,\sqrt{5})$ for $d_{P,min}$.

The first row of the rotation matrix is reported in Table III. The entire matrix can be easily obtained by the construction given in the previous section.

n	index					$d_{P,min}$
3	1–3	-0.3199	0.7189	0.5765		
	4–6	-0.0590	0.1326	0.1654		$1.825\ 10^{-3}$
8	1–4	0.0583	-0.0943	0.1407	-0.2277	
	5–8	0.1926	-0.3116	0.4649	-0.7522	$3.685\ 10^{-6}$
12	1–4	-0.1517	0.3409	-0.2734	0.0938	
	5–8	-0.2107	0.1690	0.2751	0.4721	
	9–12	0.0333	-0.0869	0.2317	0.5860	$1.528\ 10^{-10}$

TABLE III

First rows of the generator matrices of $Z_{6,6}$, $Z_{8,8}$ and $Z_{12,12}$

C.3 Other dimensions

In all the previous cases we were able to obtain the closed form expressions for the optimal rotation matrices. If we further increase the dimension a greater number of constraints become non linear and the degree of the polynomial equations giving the optimal values of λ becomes greater than four, which is the ultimate limit for closed form solutions.

In these cases we adopt a purely numerical approach to find the peek values of $d_{P,min}$. Unfortunately we are not able to guarantee the absolute optimality of the rotations. We report in Table III the numerical values of the first row of the rotation matrix for dimensions 8 and 12. The entire matrices can be easily reconstructed by iterating the construction given in the previous sections.

VII. Simulation results

In this section we give a complete presentation of the performance curves of the rotated constellations that we have constructed in the previous sections.

We first consider a throughput of $\eta = 4$ bit/symbol so that we will compare the performance with a traditional 16-QAM modulation scheme. In all the figures we plot the BER

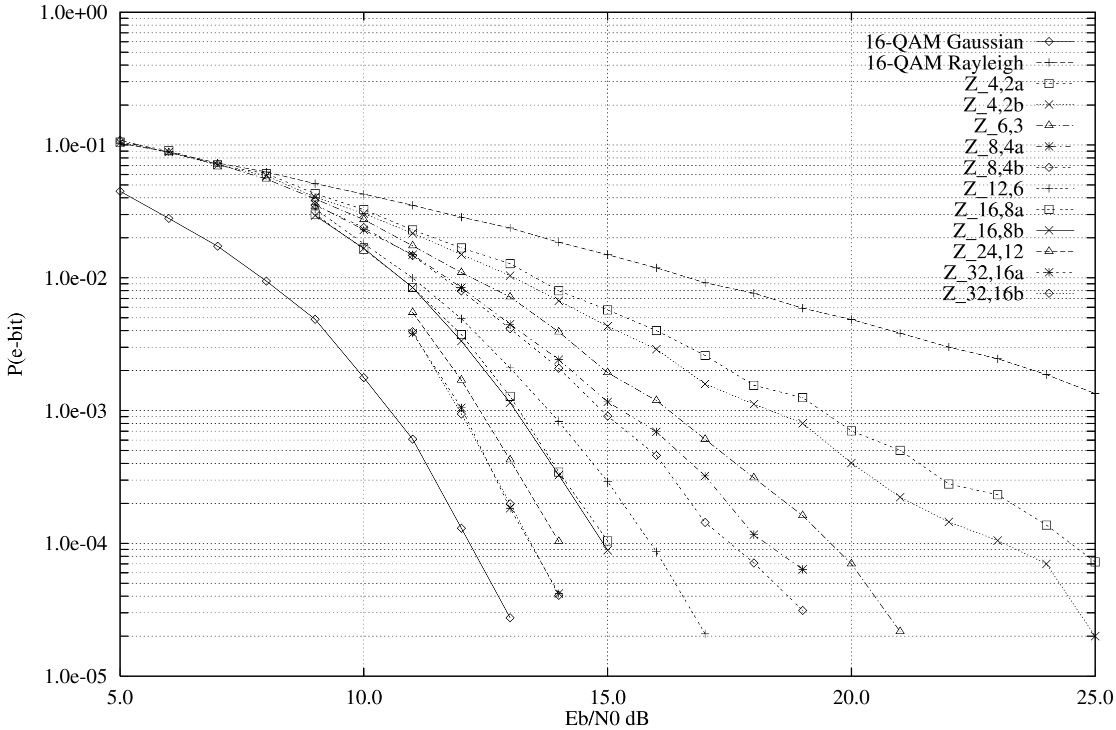

Fig. 8. Bit error rates for the family of $Z_{n,n/2}$ constellations ($\eta = 4$)

curve of the 16-QAM over the Gaussian channel and over the independent Rayleigh fading channel. These two curves bound the region of potential gain over the fading channel, when the rotated multidimensional uncoded schemes are used.

The first family of curves (Fig. 8) corresponds to constellations in dimensions n up to 32 and diversity $L = n/2$ (Sec. V-B). As the diversity increases the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is only about 1.5 dB between 10^{-3} and 10^{-4}. These constellations can be easily constructed for any dimension $n = 2^{e_1}3^{e_2}$, $e_1, e_2 = 0, 1, 2 \ldots$. The only limitation in going beyond dimension 32 is the decoder complexity.

The second family of curves (Fig. 9) corresponds to constellations in dimensions n up to 15 and diversity $L = n$ (Sec. V-C). As the diversity increases ($L = 3, 5, 9, 11, 15$) the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is about 3 dB between 10^{-3} and 10^{-4}. If we compare

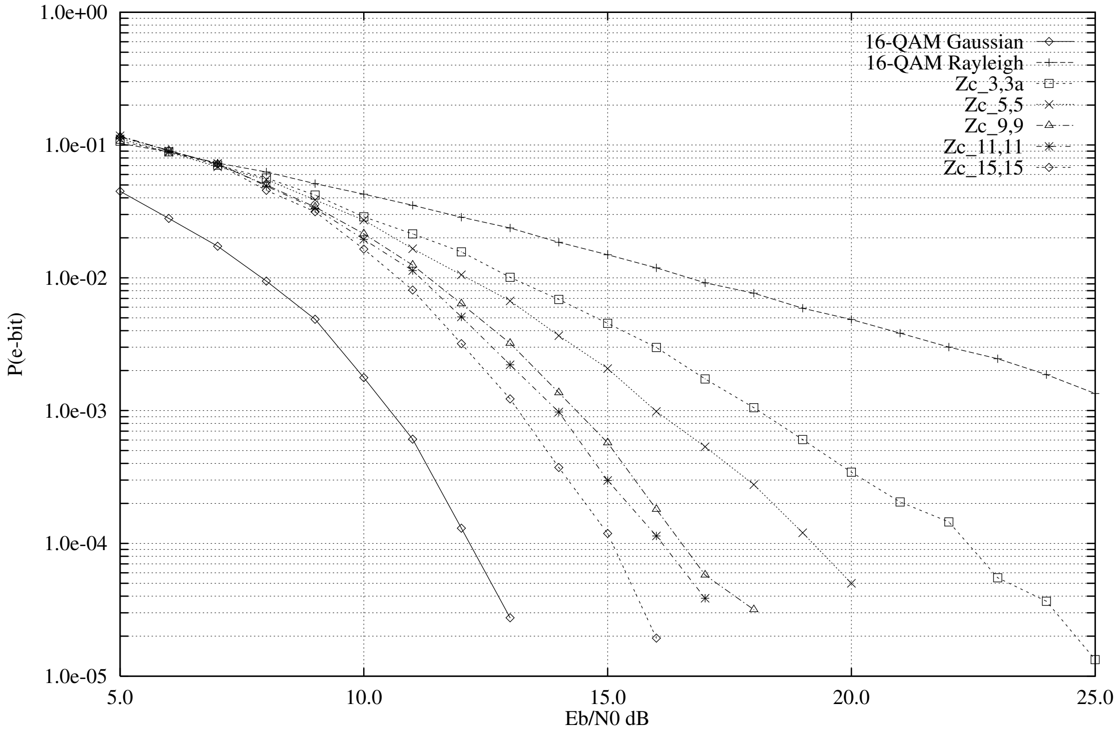

Fig. 9. Bit error rates for the family of $Z_{n,n}$ constellations from $\mathbf{Q}(2\cos(2\pi/N))$ ($\eta = 4$)

these curves with the previous ones we observe that for similar dimensions (e.g. 15 and 16) the performance is similar. This shows that the doubling of the diversity is not sufficient to increase the performance. We have verified experimentally that for these constellations the product kissing number τ_p is much larger and we believe that this is the limiting factor to improving the performance by simply increasing the diversity.

The third family of curves (Fig. 10) corresponds to constellations in dimensions n up to 12 and full diversity $L = n$ (Sec. VI). As the diversity increases ($L = 3, 4, 6, 8, 12$) the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is about 4dB between 10^{-3} and 10^{-4}. The computational complexity of finding these rotations is the limiting factor in increasing dimension. Having optimized the minimum product distance we expected a performance improvement. Unfortunately, the product kissing number is again the limiting factor. For the four-dimensional case we have plotted the curves for two distinct rotations corresponding to

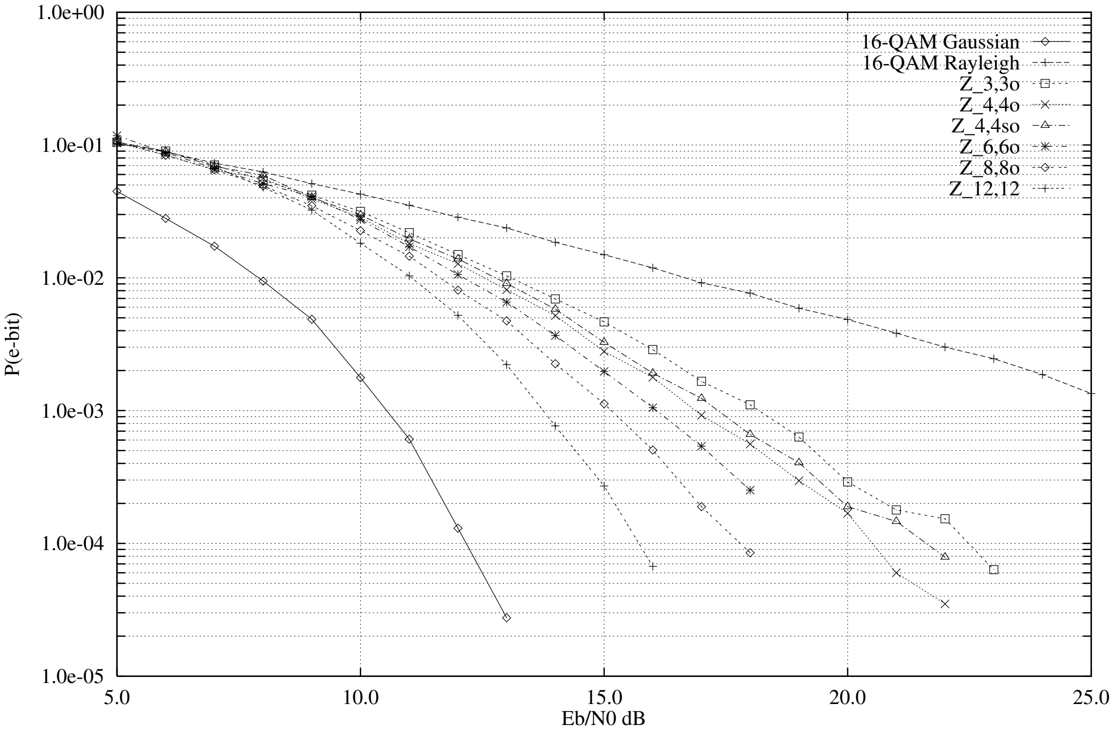

Fig. 10. Bit error rates for the family of $Z_{n,n}$ constellations which maximize the minimum product distance ($\eta = 4$)

different values of the minimum product distance (see Section VI-C.1). In this case doubling $d_{p,min}$ only improves by a few tenths of a dB.

Finally we show in Figure 11 the case of $\eta = 2$ bits/symbol which can be compared to the traditional 4-PSK modulation scheme. We considered the case of $Z_{n,n/2}$ rotations. In this case the gap to the Gaussian BER curve is less than $1\,$dB between 10^{-3} and 10^{-4}.

This figure is also useful for comparison with the coded system proposed in [8] with 2 bits/symbol. There, a rate 1/2 trellis coded rotated 16-QAM is used and BER of 10^{-4} is achieved with $E_b/N_0 = 19\,$dB. Our uncoded system provides the same performance using only a four-dimensional constellation and greater gains can be obtained by increasing the dimension.

VIII. Conclusions

In this paper we have analyzed an alternative diversity technique and we have constructed high diversity modulation schemes which exhibit an almost Gaussian performance over the

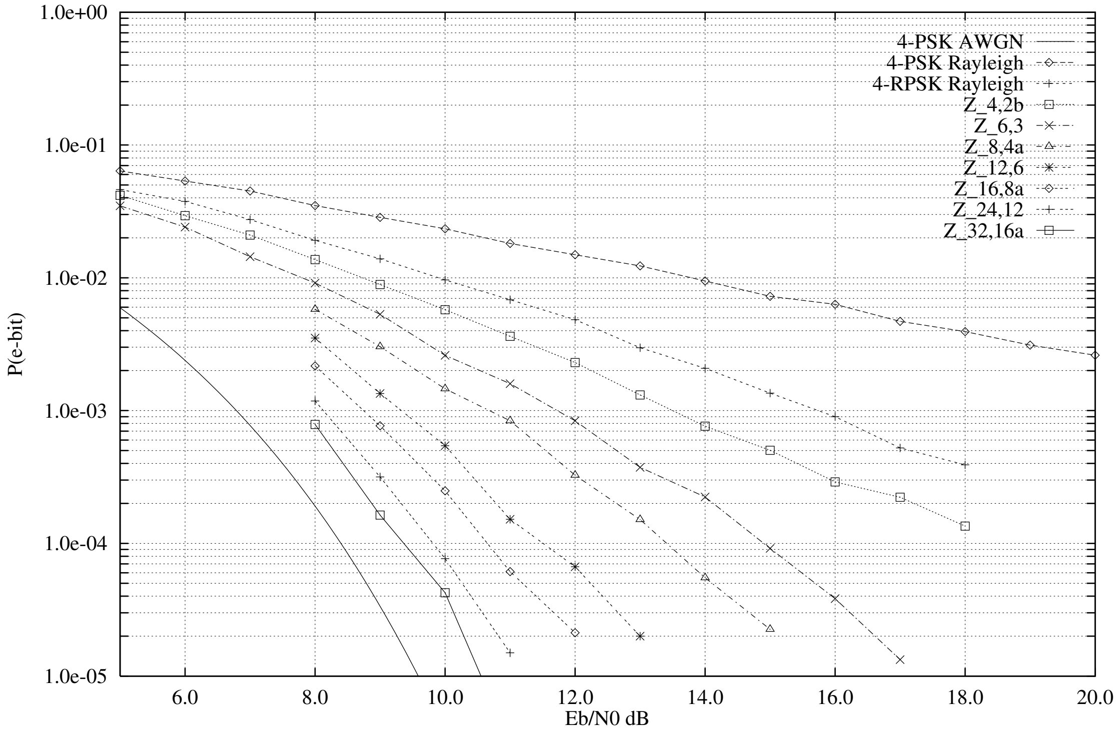

Fig. 11. Bit error rates for the family of $Z_{n,n/2}$ constellations ($\eta = 2$)

fading channel.

The great advantage of this type of diversity is that it is traded only for a higher demodulator complexity. No additional power or bandwidth is required, since no type of redundancy is added.

We have verified that the diversity order L and the minimum product distance $d_{p,min}$ are not the only important design parameters. The product kissing number τ_p is also a critical design parameter. The constellation design which takes into account τ_p is still an open problem.

Using the *Universal lattice decoder* the ML detection complexity is independent of the system throughput η: only increasing the number of dimensions slows down the demodulation operation.

Future developments of this work include the analysis of additional error control coding techniques, the effects of imperfect CSI estimation, performance analysis with correlated fading channels.

IX. Acknowledgments

The authors are grateful to Prof. Michele Elia and to Dr. Olivier Rioul for suggesting the two different proofs in the appendix. They would also like to thank the reviewers for the valuable suggestions and comments which greatly helped in improving the first version of the paper.

Appendix

I. The minimal polynomial of $2\cos(2\pi/N)$

This appendix gives two different methods to compute the minimal polynomials $\mu(x)$ of $2\cos(2\pi/N)$ for any N.

Proof 1 – Let $m(x)$ be the minimal polynomial of $\theta = e^{2\pi j/N}$ (i.e., the cyclotomic polynomial of degree $\phi(N)$) and let $x = 2\cos(2\pi/N) = \theta + 1/\theta$ then

$$\theta^2 - x\theta + 1 = 0 \quad \text{and} \quad \theta_{1,2} = \frac{x \pm \sqrt{x^2-4}}{2}$$

We now consider the polynomial with integer coefficients $g(x) = m(\theta_1)m(\theta_2)$. This polynomial has degree $\Phi(N)$ and must contain a factor of degree $\Phi(N)/2$ which is the minimal polynomial we are looking for. This implies that $g(x) = \mu(x)^2$ so that the minimal polynomial can be obtained using Euclid's algorithm to compute the greatest common divisor between $g(x)$ and its derivative $g'(x) = 2\mu(x)\mu'(x)$.

Proof 2 – Let $m(x) = \sum_{k=0}^{n} a_k x^k$ be the minimal polynomial of $\theta = e^{2\pi j/N}$ i.e., the cyclotomic polynomial of degree $n = \phi(N)$.

Using the fact that $m(x)$ is reciprocal since it also admits θ^{-1} as a root, we can write the relation $\theta^{-n/2}m(\theta) = 0$ as

$$\sum_{k=0}^{n/2} a'_{n/2-k}(\theta^k + \theta^{-k}) = 0$$

where $a'_k = a_k$ except $a'_{n/2} = a_{n/2}/2$. Noting that $(\theta^k + \theta^{-k}) = 2\cos(2\pi k/N) = T_k(\cos 2\pi/N)$

where $T_k(x)$ is the k-th Chebychev polynomial of the first kind, we obtain

$$\mu(x) = \sum_{k=0}^{n/2} a'_{n/2-k} T_k(x) = 0 \ .$$

To show that $\mu(x)$ is the minimal polynomial of $x = 2\cos(2\pi/N)$ it is enough to show that it is irreducible. Indeed, if it were reducible, then going backwards from the relation $\mu(x) = 0$ gives a non trivial factorization of $\Phi_N(\theta)$ over $\mathbf{Q}$, which is impossible.

We can conclude that the minimal polynomial of x over $\mathbf{Q}$ is given above and has degree $n/2$.

Using the above proof it is easy to show that if N is odd, since $\Phi_{2N}(\theta) = \Phi_N(-\theta)$, $\mu_{2N}(x) = \mu_N(-x)$: the minimal polynomial for $x = \cos 2\pi/2N$ is obtained from the minimal polynomial of $x = \cos 2\pi/N$ by changing the sign of x.

References

[1] S. Sampei, T. Sunaga: "Rayleigh fading compensation for QAM in land mobile radio communications," *IEEE Trans. on Veh. Technol.*, vol. 42, no. 2, May 1993, pp. 137–147.

[2] J. Du, B. Vucetic: "Trellis coded 16-QAM for fading channels," *European Trans. Telecom.*, vol. 4, no. 3, May-June 1993, pp. 335–341.

[3] D. Subasinghe-Dias, K. Feher: "A coded 16-QAM scheme for fast fading mobile radio channels," *IEEE Trans. Commun.*, vol. 43, no. 5, May 1995, pp. 1906–1916.

[4] J. Boutros, E. Viterbo, C. Rastello, J. C. Belfiore: "Good lattice constellations for both Rayleigh fading and Gaussian channel," *IEEE Trans. on Information Theory*, vol. 42, no. 2, March 1996, pp. 502–518.

[5] J. Boutros, M. Yubero: "Converting the Rayleigh fading channel into a Gaussian channel," *Mediterranean Workshop on Coding and Information Integrity*, Palma, Feb. 1996.

[6] E. Viterbo, E. Biglieri:"A universal lattice decoder," 14-ème Colloque GRETSI, Juan-les-Pins, Sept. 1993.

[7] E. Viterbo, J. Boutros:"A universal lattice code decoder for fading channels," submitted to *IEEE Trans. on Information Theory*, April 1996.

[8] B. D. Jeličić, S. Roy: "Design of a trellis coded QAM for flat fading and AWGN channels," *IEEE Trans. on Vehicular technology*, vol. 44, n. 1, Feb. 1995.

[9] J. H. Conway, N. J. Sloane: *Sphere packings, lattices and groups,* 2nd ed., 1993, Springer-Verlag, New York.

[10] K. Boullé, J. C. Belfiore: "Modulation scheme designed for the Rayleigh fading channel," CISS'92, Princeton, March 1992.

[11] J.G. Proakis: *Digital communications,* New York, McGraw Hill, 3rd edition, 1995.

[12] A. Papoulis: *Probability, random variables, and stochastic processes*, New York, McGraw Hill, 3rd edition, 1991.

[13] P. Samuel: *Algebraic theory of numbers,* Paris: Hermann 1971.

[14] S. Lang: *Algebraic Number Fields,* Addison Wesley, 1971.

[15] H. Hasse: *Number Theory,* Springer Verlag, 1980.

Biographies

Joseph Boutros (IEEE Member) was born in Beirut, Lebanon, in 1967. After his studies at Saint Joseph University (Beirut) he joined the Ecole Nationale Supérieure des Télécommunications (ENST), Paris, France, where he received an Electrical Engineering degree in 1992 and a Ph.D. degree in 1996. Since September 1996, he is with the Communications Department at ENST as an Associate Professor. His fields of interest are lattice sphere packings, algebraic number theory, parallel concatenated codes, and multicarrier transmissions. Dr. J. Boutros is a member of URA-820 of the French National Scientific Research Center (CNRS).

Emanuele Viterbo (M'95) was born in Torino, Italy, in 1966. He received his degree (Laurea) in Electrical Engineering in 1989 and his Ph.D. in 1995 in Electrical Engineering, both from the Politecnico of Torino, Torino, Italy.

From 1990 to 1992 he was with the European Patent Office, The Hague, The Netherlands, as a patent examiner in the field of dynamic recording and in particular in the field of error-control coding. Between 1995 and 1997 he held a post-doctoral position in the Dipartimento di Elettronica of the Politecnico di Torino in Communications Techniques over Fading Channels. He is currently a visting researcher in the Information Sciences Research Center of AT&T Research, Florham Park, NJ.

Dr. Emanuele Viterbo was awarded a NATO Advanced Fellowship in 1997 from the Italian National Research Council. His current research interests are in lattice codes for the Gaussian and fading channels, algebraic coding theory, digital terrestrial television broadcasting, and digital magnetic recording.

List of Figures

List of Tables

Footnote on page 7

We note that this intuitive idea is mathematically unprecise since K has the same density of $\mathbf{Q}$ in $\mathbf{R}$.