Algebraic Tools to Build Modulation Schemes for Fading Channels

Xavier Giraud, *Member, IEEE*, Emmanuel Boutillon, and Jean Claude Belfiore, *Member, IEEE*

***Abstract*—A unified framework is presented in order to build lattice constellations matched to both the Rayleigh fading channel and the Gaussian channel. The method encompasses the situations where the interleaving is done on the real components or on two-dimensional signals. In the latter case, a simple construction of lattices congruent to the densest binary lattices with respect to the Euclidean distance is proposed. It generalizes, in a sense to be clarified later, the structural construction proposed by Forney. These constellations are next combined with coset codes. The partitioning rules and the gain formula are similar to those used for the Gaussian channel.**

***Index Terms*—Coset codes, diversity, fading channels, lattices, number fields.**

I. Introduction

On a fading channel, errors occur systematically when the channel is in a deep fade. In this case, the transmitted information is lost for the receiver. However, if the receiver can be provided with several replicas of the information which have been subjected to independent fadings, an appropriate combination of the replicas can restore the information. There are several diversity techniques by which the receiver can be provided with independently fading replicas of the information-bearing signal. In the case of time diversity, the replicas of the signal are transmitted at different times. The time interval between each of these transmissions is longer than the coherence time of the channel so that for each of the transmission time slots the attenuation factors (or channel states) can be considered as independent. Analogously, in frequency diversity, the signal is transmitted on different frequency bands separated by at least the coherence bandwidth. In both cases, the diversity techniques can be represented as repetition coding and interleaving in time and frequency of the replicas. These methods improve the error rate at the expense of spectral efficiency. We have introduced in [1] a new approach for designing signal sets at high signal-to-noise ratio (SNR). This method has no detrimental effect on spectral efficiency and it provides the receiver with an order of diversity dependent on the number of dimensions of the symbol constellation. It is based on a geometric formulation of the constellation design problem. The sphere packing formulation for the Gaussian channel is produced as a special case and the results given by this approach for the Rayleigh fading channel (RFC) were first presented in [2]. Specifically, we have shown that the design lattice problem is tantamount to the determination of an admissible lattice of a body S dependent on the channel. A lattice Λ is S-admissible when $S \cap \Lambda = \{\mathbf{0}\}$ where $\mathbf{0}$ is the origin. In the Gaussian case, S is a sphere. When specialized to the case of a perfectly interleaved/de-interleaved Rayleigh fading channel with ideal channel state information, a suitable upper bound on the pairwise error probability gives

$$S_r = \left\{ \boldsymbol{x} = (x_1, \cdots, x_n) \in \boldsymbol{R}^n, \quad \left| \prod_{i=1}^{n} x_i \right| \leq 1 \right\}$$

when the interleaving is performed over coordinates, and

$$S_c = \left\{ \boldsymbol{x} = (x_1, \cdots, x_n) \in \boldsymbol{C}^n, \quad \prod_{i=1}^{n} (a_i^2 + b_i^2) \leq 1 \right\}$$

where $x_i = a_i + jb_i$ when the interleaving is performed on two–dimensional (2-D) symbols.

Admissibility for a lattice is desirable because it guarantees that any constellation carved out of Λ offers an nth-order diversity on the Rayleigh fading channel. In this paper, we give a unified construction for S_r- and S_c-admissible lattices. In Section V, we show in which way n-dimensional lattice constellations, matched for both the Rayleigh fading channel and the Gaussian channel, can be built with full diversity on the fading channel. These constellations are S_r-admissible. In Section VI, we give an alternative construction to the one proposed in [14] in order to build S_c-admissible lattices congruent to the densest lattices with respect to the Euclidean distance, i.e., good lattices on the Gaussian channel. They yield an $n/2$th-order diversity. The construction does not need advanced tools from number field theory and follows the structural construction proposed by Forney in [5].

Coset codes have been used on the Rayleigh fading channel in order to increase the diversity order. Since diversity can be obtained with properly designed lattice constellations, we would rather combine admissible constellations on the Rayleigh fading channel with coset codes in a similar way as for the Gaussian channel. In Section VII, the partitioning rules and the coding gain are studied and the theoretical results are compared with computer simulations.

II. Admissible Signal Set

Let C be the constellation containing the two n-dimensional signal points $\boldsymbol{x}$ and $\boldsymbol{t}$ only. At the output of the transmission channel, upon observation of the n-dimensional vector $\boldsymbol{y}$, the

Manuscript received August 31, 1995; revised October 10, 1996. The material in this paper was presented in part at the IEEE 1993 International Symposium on Information Theory, San Antonio, TX, at the IEEE 1994 International Symposium on Information Theory, Trondheim, Norway, and at the 1996 Information Theory Workshop, Haifa, Israel.

The authors are with Ecole Nationale Supérieure des Télécommunications, Département Communications, 75634 Paris Cedex 13 France.

Publisher Item Identifier S 0018-9448(97)02639-4.

decision on the transmitted signal is based on the maximization of a metric $m(\boldsymbol{u}, \boldsymbol{y})$ with $\boldsymbol{u} \in C$. Under this decision rule, we may define the pairwise error probability $p(\boldsymbol{x} \to \boldsymbol{t})$ as the probability that $m(\boldsymbol{t}, \boldsymbol{y})$ is larger than $m(\boldsymbol{x}, \boldsymbol{y})$ when $\boldsymbol{x}$ is transmitted. Finally, we introduce the mapping $\tilde{p}$ on $F^n \times F^n$ where $F = \boldsymbol{R}$ or $F = \boldsymbol{C}$

$$\tilde{p}: \begin{cases} (\boldsymbol{x}, \boldsymbol{t}) \mapsto p(\boldsymbol{x} \to \boldsymbol{t}), & \text{if } \boldsymbol{x} \neq \boldsymbol{t} \\ (\boldsymbol{x}, \boldsymbol{t}) \mapsto +1, & \text{if } \boldsymbol{x} = \boldsymbol{t}. \end{cases}$$

We take liberty in referring to $\tilde{p}$ as the pairwise error probability function.

Let $C = (\boldsymbol{x}_i)_{i \in I}$, I, an index set, be a finite signal set with $|I|$ equiprobable signals. If the pairwise error probability $p(\boldsymbol{x}_i \to \boldsymbol{x}_j)$ between any two different signals is smaller than ε then, by means of the union bound, the symbol error probability is upper-bounded by

$$P_S \leq \frac{1}{|I|} \sum_{i \neq j} p(\boldsymbol{x}_i \to \boldsymbol{x}_j) \leq |I| \times \varepsilon.$$

Considering this bound, a signal set C is said to be "ε-admissible" if for any pair $\boldsymbol{x}, \boldsymbol{t} \in C$, the pairwise error probability $p(\boldsymbol{x} \to \boldsymbol{t})$ is smaller than ε.

Let $\boldsymbol{x} \in F^n$ be an arbitrary n-dimensional point. By means of the mapping $\tilde{p}$ we define the set of the nonadmissible points with respect to $\boldsymbol{x}$ as

$$S_x^\varepsilon = \{\boldsymbol{t} \in F^n,\ \tilde{p}(\boldsymbol{x}, \boldsymbol{t}) > \varepsilon\}.$$

We assume in the following that S_x^ε is an open set, if it is not the case, then we take its topological interior. With these notations, the signal set C is ε-admissible if each region $S_x^\varepsilon, \boldsymbol{x} \in C$, contains only one signal from C, this signal being $\boldsymbol{x}$.

$$S_x^\varepsilon \cap C = \{\boldsymbol{x}\}$$

A. Geometrical Properties

Before we tailor our analysis to the Rayleigh fading channel, we will discuss in greater detail the concept of admissibility. We show here how most of the ideas introduced by Forney in [4] can be translated in terms of admissible constellations. This is not surprising since both concepts are geometrical and it points to a construction technique similar to that of geometrically uniform signal sets.

Let G be the set of permutations of the n-dimensional vector space F^n leaving the pairwise error probability unchanged.

$$\forall f \in G \quad \forall \boldsymbol{x}, \boldsymbol{s} \in F^n \quad \tilde{p}(f(\boldsymbol{x}), f(\boldsymbol{s})) = \tilde{p}(\boldsymbol{x}, \boldsymbol{s}).$$

$(G, \circ)$ is a subgroup of the group of the permutations of F^n under composition.

When the Gaussian channel is considered, $\tilde{p}(\boldsymbol{x}, \boldsymbol{s})$ is a function of the Euclidean distance $||\boldsymbol{x} - \boldsymbol{s}||_2$ between $\boldsymbol{x}$ and $\boldsymbol{s}$. Consequently, the elements of G are the isometries of $\boldsymbol{R}^n$ and S_x^ε is the open ball centered at $\boldsymbol{x}$ with radius depending on ε and on the variance of the noise.

If $\boldsymbol{x} \in \boldsymbol{R}^n$ and f is in G then the set of nonadmissible points with respect to $\boldsymbol{x}$ and the set of nonadmissible points with respect to $f(\boldsymbol{x})$ are closely related. In fact, we have

Proposition 1:

$$\forall f \in G \quad \forall x \in F^n \quad S_{f(x)}^\varepsilon = f(S_x^\varepsilon).$$

Proof:

$$\begin{aligned} \boldsymbol{t} \in S_{f(x)}^\varepsilon &\Leftrightarrow \tilde{p}(f(\boldsymbol{x}), \boldsymbol{t}) > \varepsilon \\ &\Leftrightarrow \tilde{p}(f(\boldsymbol{x}), f(f^{-1}(\boldsymbol{t}))) > \varepsilon \\ &\Leftrightarrow \tilde{p}(\boldsymbol{x}, f^{-1}(\boldsymbol{t})) > \varepsilon \\ &\Leftrightarrow f^{-1}(\boldsymbol{t}) \in S_x^\varepsilon \\ &\Leftrightarrow \boldsymbol{t} \in f(S_x^\varepsilon). \end{aligned}$$ ■

Based on this property, we are now in a position to build an admissible constellation. Let H be a subgroup of G and $\boldsymbol{x}_0 \in F^n$ an arbitrary fixed point. The orbit of $\boldsymbol{x}_0$ under the action of H is defined as

$$H.\boldsymbol{x}_0 = \{h(\boldsymbol{x}_0), h \in H\}.$$

We have

Proposition 2: The signal set $H.\boldsymbol{x}_0$ is admissible if and only if $H.\boldsymbol{x}_0 \cap S_{x_0}^\varepsilon = \{\boldsymbol{x}_0\}$.

Proof: The direct implication is obvious. For the converse, let $\boldsymbol{x} \in H.\boldsymbol{x}_0$, we have $\boldsymbol{x} = h(\boldsymbol{x}_0)$ for some h in H and

$$\begin{aligned} S_x^\varepsilon \cap H.\boldsymbol{x}_0 &= h(S_{x_0}^\varepsilon) \cap H.\boldsymbol{x}_0 = h(S_{x_0}^\varepsilon \cap H.\boldsymbol{x}_0) \\ &= \{h(\boldsymbol{x}_0)\} = \{\boldsymbol{x}\} \end{aligned}$$

because $hH = H$. Hence, $H.\boldsymbol{x}_0$ is admissible. ■

Proposition 2 asserts that the admissibility at $\boldsymbol{x}_0$ is tantamount to the admissibility of $H.\boldsymbol{x}_0$. Besides, if H is a normal subgroup of G and $H.\boldsymbol{x}_0$ is admissible then $H.g(\boldsymbol{x}_0)$ is also admissible whichever $g \in G$ is considered, i.e., if the "center" of the constellation is moved to another point of $G.\boldsymbol{x}_0$, we still obtain an admissible constellation. When G reduces to the set of translations, a subgroup H of G such that $H.\boldsymbol{o}$ is admissible should be obtained ($\boldsymbol{o}$ is the origin).

B. Translation Invariance

We specialize our analysis to the case of a mapping $\tilde{p}$ which is translation-invariant.

$$\forall \boldsymbol{x}, \overrightarrow{\boldsymbol{u}}, \boldsymbol{t} \in F^n \quad \tilde{p}(\boldsymbol{x} + \overrightarrow{\boldsymbol{u}}, \boldsymbol{t} + \overrightarrow{\boldsymbol{u}}) = \tilde{p}(\boldsymbol{x}, \boldsymbol{t})$$

so that from Proposition 1, we have $S_{x'}^\varepsilon = S_x^\varepsilon + \overrightarrow{\boldsymbol{x}\boldsymbol{x}'}$.

1) The Packing Formulation: Let S be an open subset of F^n. The system consisting of the translates $(S + \boldsymbol{x})_{\boldsymbol{x} \in C}$ is called a (S, C)-packing of S if for any two distinct points $\boldsymbol{x}, \boldsymbol{t} \in C$, the sets $\boldsymbol{x} + S$ and $\boldsymbol{t} + S$ are disjoint. We assume now that $S_{\boldsymbol{o}}^\varepsilon$ is open, bounded, *convex*, and $\boldsymbol{o}$-symmetric, i.e., $(-\boldsymbol{x}, \boldsymbol{x}) \subset S_{\boldsymbol{o}}^\varepsilon$ for all $\boldsymbol{x} \in S_{\boldsymbol{o}}^\varepsilon$.

Proposition 3: A signal set C, finite or not, is ε-admissible if and only if $(\frac{1}{2} S_{\boldsymbol{o}}^\varepsilon, C)$ is a packing of $\frac{1}{2} S_{\boldsymbol{o}}^\varepsilon$.

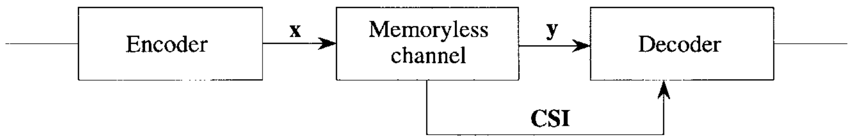


Fig. 1. A general baseband transmission model.

Proof:

$$\forall \boldsymbol{x}, \boldsymbol{t} \in F^n \quad (\boldsymbol{x} + \tfrac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}) \cap (\boldsymbol{t} + \tfrac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}) \neq \emptyset \Leftrightarrow \boldsymbol{t} - \boldsymbol{x} \in S^{\varepsilon}_{\boldsymbol{o}} \Leftrightarrow \boldsymbol{t} \in \boldsymbol{x} + S^{\varepsilon}_{\boldsymbol{o}} \Leftrightarrow \boldsymbol{t} \in S^{\varepsilon}_{x}.$$

Suppose that C is S-admissible and let $\boldsymbol{x}$ and $\boldsymbol{t}$ be two distinct points in C then $\boldsymbol{t} \notin S^{\varepsilon}_{\boldsymbol{x}}$, hence,

$$(\boldsymbol{x} + \tfrac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}) \cap (\boldsymbol{t} + \tfrac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}) = \emptyset.$$

Therefore, $(\frac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}, C)$ is a packing of $\frac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}$. The converse is similar. ■

Consequently, the constellation design problem for the Gaussian channel is tantamount to the sphere packing problem at high SNR since this channel is translation invariant and the Euclidean ball S^{ε}_{x} is convex and $\boldsymbol{o}$-symmetric.

2) The Lattice Design Problem: In view of Proposition 2, we restrict ourselves to signal sets carved out of lattices in order to draw benefit from the translation invariance and we have

Proposition 4: A lattice Λ, i.e., a discrete subgroup of $(F^n, +)$, or any of its translates $\boldsymbol{x} + \Lambda$ is ε-admissible if and only if $S^{\varepsilon}_{\boldsymbol{o}} \cap \Lambda = \{\boldsymbol{o}\}$.

In order to minimize energy, we want to maximize the number of lattice points per unit volume. This is obtained by choosing an $S^{\varepsilon}_{\boldsymbol{o}}$-admissible lattice of which the determinant is minimum.

Admissibility is a notion borrowed from the geometry of numbers [7]. When $S^{\varepsilon}_{\boldsymbol{o}}$ is $\boldsymbol{o}$-symmetric, Malher's selection theorem asserts that if there exists an $S^{\varepsilon}_{\boldsymbol{o}}$-admissible lattice, then there exists an $S^{\varepsilon}_{\boldsymbol{o}}$-admissible lattice with minimal determinant, called a critical lattice of $S^{\varepsilon}_{\boldsymbol{o}}$. Such a lattice is not necessarily unique. Hence in the language of the geometry of numbers, *the lattice design problem is tantamount to determining a critical lattice of $S^{\varepsilon}_{\boldsymbol{o}}$ provided that $S^{\varepsilon}_{\boldsymbol{o}}$ is $\boldsymbol{o}$-symmetric.*

If in addition, $S^{\varepsilon}_{\boldsymbol{o}}$ is convex, a critical lattice of $S^{\varepsilon}_{\boldsymbol{o}}$ achieves the maximum density of a lattice packing of $\frac{1}{2} S^{\varepsilon}_{\boldsymbol{o}}$ as a consequence of Proposition 3. In the Gaussian case, for example, our formulation reduces to the lattice packing of spheres.

III. A Case of Study: The Fading Channels

A. The Pairwise Error Probability

A general transmission model is shown in Fig. 1. Corresponding to the input vector $\boldsymbol{x} = (x_1, \cdots, x_n)$, the channel outputs the sequence $\boldsymbol{y}$ whose kth coordinate is related to x_k by

$$y_k = \alpha_k x_k + w_k$$

where

- α_k is a random amplitude describing the slow fading effect. We assume that the random fading phase has been compensated for. The amplitude α_k is Rician-distributed with normalized probability density function
$$\rho(x) = \begin{cases} \dfrac{x}{b} \exp\left(-\dfrac{x^2 + A^2}{2b}\right) I_0\left(\dfrac{xA}{b}\right), & x > 0 \\ 0, & \text{elswhere} \end{cases}$$
and $A^2 + 2b = 1$. The model is characterized by the ratio $K = A^2/2b$. When $A = 0$, we have the Rayleigh statistical model and when $A = 1$, we obtain the AWGN model.
- w_k is a sample of a zero-mean white Gaussian noise process. The components are either real or complex zero-mean values with variance σ^2 in the real case and $2\sigma^2$ in the complex case.

The channel input alphabet comprises M signal symbols with average energy per dimension $\overline{E}$. The signal-to-noise ratio is then defined as

$$\Gamma = \frac{\overline{E}}{2\sigma^2}.$$

We assume that the channel is memoryless by means of perfect interleaving/de-interleaving. The components are real, i.e., $x_i \in \boldsymbol{R}$, when the interleaving is performed at the coordinate level and complex, i.e., $x_i \in \boldsymbol{C}$, when the interleaving is done over the complex symbols. After de-interleaving and when the channel state information is ideally known, the maximum-likelihood detection involves the minimization of the following metric:

$$m(\boldsymbol{t}, \boldsymbol{y}) = \sum_{i=1}^{n} |y_i - \alpha_i t_i|^2$$

over all the vectors $\boldsymbol{t}$ in the constellation. The Chernoff bound technique proposed by Divsalar and Simon [8] can be used to upper-bound the pairwise error probability, which leads to

$$p(\boldsymbol{x} \to \boldsymbol{s}) \leq f(K, \boldsymbol{u}) \tag{1}$$

where

$$f(K, \boldsymbol{u}) = \prod_{i=1}^{n} \frac{1 + K}{1 + K + |u_i|^2} \exp\left(-\frac{K|u_i|^2}{1 + K + |u_i|^2}\right)$$
$$u_i = \sqrt{\frac{\Gamma}{4\overline{E}}}|x_i - s_i|.$$

The notation $|x|$ denotes the absolute value or the modulus, depending on whether $x \in \boldsymbol{R}$ or $x \in \boldsymbol{C}$. When $A = 0$ (Rayleigh channel) (1) simplifies to

$$p(\boldsymbol{x} \to \boldsymbol{s}) \leq \prod_{i=1}^{n} \frac{1}{1 + |u_i|^2}. \tag{2}$$

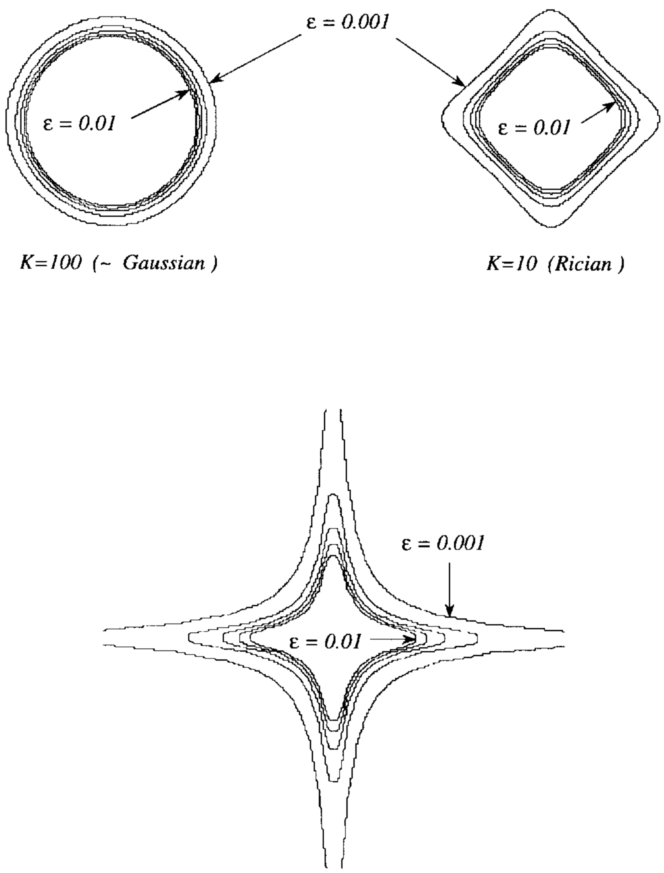


Fig. 2. Behavior of S_ε.

When $A = 1$ (AWGN channel), (1) is the Bhattacharyya bound.

Although (1) is not the exact expression of the pairwise error probability, the framework of Section II is applicable but the performance may not be optimal. The function $f(K, \boldsymbol{u})$ may be viewed as the pairwise error probability of some fictitious channel worse than the fading channel. In this respect, an admissible constellation for the fictitious channel is admissible for the fading channel. In view of Section II-B, we look for a critical lattice of the star body

$$S_K^\varepsilon = \{\boldsymbol{x} \in F^n, f(K, \boldsymbol{u}) > \varepsilon\}, \qquad \text{where} \quad F = \boldsymbol{R} \text{ or } \boldsymbol{C}.$$

The size of S_K^ε is actually larger than needed. Fig. 2 represents the curve $f(K, \boldsymbol{u}) = \varepsilon$ for different values of K with $10^{-3} \le \varepsilon \le 10^{-2}, n = 2$ and real components. Observe that S_K^ε is not necessarily convex; in that case, we remind that the packing formulation does not apply.

B. The Lattice Design Problem

1) Asymptotic Values:

- When K approaches infinity (Gaussian channel), the body S_K^ε is a sphere and we have already mentioned in Section II-B that the lattice design problem is tantamount to the lattice packing of spheres.
- If the shadowing is severe and K approaches 0, the body S_K^ε is a scaled version of
$$S^\varepsilon = \left\{\boldsymbol{x} \in F^n, \prod_{i=1}^n (|x_i|^2 + \varepsilon^{1/n}) < 1\right\}$$
where $F = \boldsymbol{R}$ when the interleaving is performed over coordinates and $F = \boldsymbol{C}$ when it is done on 2-D symbols.

Observe that $S^\varepsilon \subset S$ where

$$S = \left\{\boldsymbol{x} \in F^n, \prod_{i=1}^n |x_i|^2 < 1\right\}.$$

If Λ is S-admissible, then it is S^ε-admissible and S^ε goes to S as ε decreases. Besides, any pair of channel symbols picked out of Λ have all their coordinates distinct in F, hence any constellation carved out of the lattice Λ provides an nth-order diversity, i.e., the pairwise error probability varies inversely with Γ^n. At low error rate, the design of a lattice matched to the Rayleigh fading channel reduces to finding a critical lattice of S.

If the components are real (interleaving over the coordinates), we write

$$S_r = \left\{\boldsymbol{x} \in \boldsymbol{R}^n, \left|\prod_{i=1}^n x_i\right| \le 1\right\}. \tag{3}$$

When the interleaving is performed on 2-D symbols, we write

$$S_c = \left\{\boldsymbol{x} \in \boldsymbol{C}^n, \prod_{i=1}^n (a_i^2 + b_i^2) \le 1\right\} \tag{4}$$

where $x_k = a_k + ib_k$ with i standing for $\sqrt{-1}$.

The effective construction of an S-admissible lattice is not easy. Techniques from number theory are proposed to overcome this difficulty. This problem is treated in Section IV.

2) The Rician Channel $(0 < K < \infty)$*:* The characteristic of the Rician fading channel lies between the Gaussian channel and the Rayleigh fading channel. When the components are *real*, this intermediate position is illustrated by Fig. 2. When $K = 10$, it clearly suggests to approximate the set of nonadmissible points with respect to the origin by a diamond

$$P_2 = \{(x, y) \in \boldsymbol{R}^2, |x| + |y| < 1\}.$$

A critical lattice of the diamond is

$$\Re \boldsymbol{Z}^2 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \boldsymbol{Z}^2.$$

The corresponding packing density gain over $\boldsymbol{Z}^2$ with respect to the ℓ_1-norm is 3 dB. Indeed, the lattice $\Re\boldsymbol{Z}^2$ yields about 3-dB gain over $\boldsymbol{Z}^2$ on the Rician channel when $K = 10$. The n-dimensional crosspolytope is

$$P_n = \left\{(x_1, \cdots, x_n) \in \boldsymbol{R}^n, \sum_{i=1}^n |x_i| < 1\right\}.$$

P_n is the unit ball for the ℓ_1-norm. As such it is convex. A good lattice for the Rician channel is expected to be a dense packing lattice of crosspolytopes, i.e., a dense lattice with respect to the ℓ_1-norm. Construction of such lattices and their performance on the Rician channel are studied in [9], [2], [10].

IV. A Family of S-Admissible Lattices

The algebraic norm at first appears in solving problems such as simple cases of the Fermat theorem, for example, *find all integer solutions of* $x^p + y^p = z^p$, *for* $p = 2$. The introduction of the number field $\boldsymbol{Q}[i] = \{a + ib, (a, b) \in \boldsymbol{Q}^2\}$ turns the problem into a multiplicative one in the ring of Gaussian integers $\boldsymbol{Z}[i] = \{a + ib, (a, b) \in \boldsymbol{Z}^2\}$. Besides, it is usual to represent $\boldsymbol{Z}[i]$ by its embedding in the two dimensional real space $\boldsymbol{R}^2$. Actually, these two facts are tightly related and can be generalized in higher dimension. These are the key ideas of what follows. The lattice design problem leads us to consider a multiplicative expression on F^n as given by (3) and (4). For each point $\boldsymbol{x} = (x_1, \cdots, x_n) \in F^n$, we set

$$N(\boldsymbol{x}) = x_1 \times \cdots \times x_n.$$

In fact, this expression looks as if it were contrived to agree with the field norm, the analog of the modulus in $\boldsymbol{Q}[i]$ as we shall see. We first review some basic definitions from field theory and we give the key results needed for the construction that we propose. Some of them are far from easy even though they may look natural to a certain extent. Proofs can be found in [11], [12].

A. Some Useful Definitions and Results

In what follows F is always the field $\boldsymbol{R}$ of real numbers or the field $\boldsymbol{C}$ of complex numbers. The capital letter R denotes the ring $\boldsymbol{Z}$ of ordinary integers when $F = \boldsymbol{R}$ and $\boldsymbol{Z}[i]$ or $\boldsymbol{Z}[j] = \{a + bj, (a, b) \in \boldsymbol{Z}^2\}$ with $j \stackrel{\text{def}}{=} e^{2i\pi/3}$ if $F = \boldsymbol{C}$. Whatever the situation here, the ring R is Euclidean. Finally K denotes the quotient field of R, i.e.,

R	$\boldsymbol{Z}$	$\boldsymbol{Z}[i]$	$\boldsymbol{Z}[j]$
K	$\boldsymbol{Q}$	$\boldsymbol{Q}[i]$	$\boldsymbol{Q}[j]$

A field L is said to be an extension of K provided that K is a subfield of L. An element $\theta \in \boldsymbol{C}$ is said to be algebraic over K provided that θ is the root of some nonzero polynomial $P \in K[X]$, the ring of polynomials with coefficients in K. If P can be chosen monic with coefficients in R, the number θ is integral over R. Apart from these definitions, we need the following results.

Let θ be integral over R.

- There is an irreducible monic polynomial $M_\theta \in K[X]$ uniquely determined by the condition that $M_\theta(\theta) = 0$, and called the minimal polynomial of θ.
- If $n = \deg M_\theta$, the polynomial M_θ has n distinct roots in $\boldsymbol{C}$, denoted by $\theta_1, \cdots, \theta_n$.

  Let $\theta = e^{i\pi/4}$; it is an integral over $\boldsymbol{Z}$ and over $\boldsymbol{Z}[i]$ as a root of $X^8 - 1$. However, the minimal polynomial of θ depends on R. If we set $R = \boldsymbol{Z}$, then $M_\theta = X^4 + 1$, while over $R = \boldsymbol{Z}[i]$, we have $M_\theta = X^2 - i$.
- The set
  $$K[\theta] = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, (a_0, a_1, \cdots, a_{n-1}) \in K^n\}$$
  is an n-dimensional vector space over K with $(1, \theta, \cdots, \theta^{n-1})$ as a basis. In addition, it is an extension field of K.
- There are exactly n embeddings of K in $\boldsymbol{C}$ which fix K pointwise. Each of them is uniquely determined by sending θ to any one of its n conjugates $\theta_1, \cdots, \theta_n$
  $$\sigma_k: x = \sum_{i=0}^{n-1} x_i\theta^i \mapsto \sigma_k(x) = \sum_{i=0}^{n-1} x_i\theta_k^i.$$

By means of these embeddings two mathematical objects relevant for our problem can be built:

- a mapping $\sigma: K[\theta] \to \boldsymbol{C}^n$ is obtained by sending each $\phi \in K[\theta]$ on the n-tuple $(\sigma_1(\phi), \cdots, \sigma_n(\phi))$. This mapping is an additive homomorphism with trivial kernel. As such, it preserves the additive structure and the dimension. Hence, an R-module of rank n in K is mapped onto an R-module of rank n in $\boldsymbol{C}^n$.
- the norm of $\phi \in K$ is defined as
  $$N(\phi) = \sigma_1(\phi) \times \cdots \times \sigma_n(\phi).$$

As we mentioned before, the mapping σ and the algebraic norm should be compared with the canonical embedding of $\boldsymbol{Q}[i]$ in $\boldsymbol{C}$ and the modulus. Proposition 5 is central to our construction. Its proof can be found in [11] when $R = \boldsymbol{Z}$ and it is generalized in [12].

Proposition 5:

Let $\mathcal{O}$ be the set of elements of $K[\theta]$ which are integral over R. Then

i) the norm of $\phi \in \mathcal{O}\backslash\{0\}$ is an element of $R\backslash\{0\}$;
ii) $\mathcal{O}$ is a ring, called the number ring of $K[\theta]$ over R;
iii) $\mathcal{O}$ is a free module of rank n over R.

B. Two Cases of Interest

- When $R = \boldsymbol{Z}$ and $\boldsymbol{Q}[\theta]$ is totally real, i.e., when $\theta_1, \cdots, \theta_n$ are real numbers, then σ ranges in $\boldsymbol{R}^n$ and Proposition 5 states that
  - ▹ the norm of $\phi \in \mathcal{O}\backslash\{0\}$ is an nonzero ordinary integer, hence
    $$|N(\phi)| = |\sigma_1(\phi) \times \cdots \times \sigma_n(\phi)| \geq 1.$$
  - ▹ $\sigma(\mathcal{O})$ is a free module of rank n over $\boldsymbol{Z}$, i.e., a lattice of $\boldsymbol{R}^n$, denoted by $\Lambda_{\mathcal{O}}$.

Combining these two results, we obtain that the embedding of the number ring of a totally real number field of degree n is S_r-admissible. The densest lattices obtained by this way are given in [1]. Simulation results confirm that the constellations carved out of such lattices offer an nth-order diversity and lead to considerable gain over $\boldsymbol{Z}^n$ on the Rayleigh fading channel.

- In the case that $R = \boldsymbol{Z}[i]$ or $\boldsymbol{Z}[j]$, we have
  - ▹ the norm of $\phi \in \mathcal{O}\backslash\{0\}$ belongs to R and it is nonzero, hence
    $$|N(\phi)| = |\sigma_1(\phi) \times \cdots \times \sigma_n(\phi)| \geq 1$$

because the modulus of a nonzero Gaussian integer or of a nonzero Eisenstein integer is a nonzero ordinary integer.

- ▷ $\sigma(\mathcal{O})$, denoted by $\Lambda_{\mathcal{O}}$, is a free module of rank n over R, i.e., it can be written as $\sigma(\mathcal{O}) = AR^n$ where A is an $n \times n$ invertible matrix with complex coefficients, called a generating matrix of $\sigma(\mathcal{O})$.

Using these two results, we have obtained a family of S_c-admissible lattices. A mapping $\boldsymbol{C}^n \to \boldsymbol{R}^{2n}$ is obtained by sending each n-tuple of complex numbers $(z_1, \cdots, z_n)$ where $z_k = x_k + iy_k$ to the $2n$-tuple of real numbers $(x_1, y_1, x_2, y_2, \cdots, x_n, y_n)$. When $R = \boldsymbol{Z}[i]$ or $R = \boldsymbol{Z}[j]$, this mapping can be applied to $\Lambda_{\mathcal{O}}$; it yields a lattice of $\boldsymbol{R}^{2n}$ denoted by $\Lambda_{\mathcal{O},r}$. A constellation carved out of $\Lambda_{\mathcal{O},r}$ yields an nth-order diversity on the Rayleigh fading channel. In Section VI we propose an alternative construction to the method initiated by Craig [13] and applied by Boutros *et al.* [14] in order to build rotated versions of the densest lattices with respect to the Euclidean norm.

V. Of S_r-Admissible Lattice

The foregoing development could be made more general. Since the proposed applications are restricted to the situation where interleaving is performed at the coordinate level, we specialize it to S_r-admissible lattices. The embedding $\Lambda_{\mathcal{O}}$ of the number ring $\mathcal{O}$ of a totally real number field yields an S_r-admissible lattice with low sphere packing density as pointed out in [2]. This consideration has motivated Boutros *et al.* to relax the requirement on diversity and investigate S_c-admissible lattices, the diversity of which is halved when compared to S_r-admissible lattices. They built a rotated version of the densest lattices with respect to the Euclidean distance out of which they carved constellations with good properties on both the Gaussian channel (a high sphere packing density) and the Rayleigh fading channel (an $n/2$th-order diversity). This section is aimed at finding a way to increase the sphere packing density of S_r-admissible lattices in order to build constellations with good properties on the Gaussian channel (a high sphere packing density) and an nth-order diversity on the Rayleigh fading channel. For this purpose, we characterize equivalent lattices on the Rayleigh fading channel and we show that inside the set of the lattices equivalent to $\Lambda_{\mathcal{O}}$, the lattice $\Lambda_{\mathcal{O}}$ is the worst regarding the sphere packing density. These facts naturally point to a lattice equivalent to $\Lambda_{\mathcal{O}}$ with maximal sphere packing density. The method is illustrated by several examples.

A. Equivalent Lattices on the Rayleigh Fading Channel (RFC)

An S_r-admissible lattice Λ with generating matrix $A = (a_{ij})$ is such that

$$\forall \boldsymbol{x} = (x_1, \cdots, x_n) \in \boldsymbol{R}^n \backslash \{\boldsymbol{o}\} \quad \prod_{i=1}^{n} |a_{i1}x_1 + \cdots + a_{in}x_n| \geq 1.$$

Let $\pi_n: (x_1, \cdots, x_n) \mapsto x_1 \times \cdots \times x_n$. An $n \times n$ matrix $A = (a_{ij})$ determines a homogeneous form of degree n defined by

$$\pi_n \circ A: (x_1, \cdots, x_n) \mapsto \prod_{i=1}^{n} (a_{i1}x_1 + \cdots + a_{in}x_n).$$

We say that two lattices Λ_1 and Λ_2 are equivalent and we write $\Lambda_1 \sim \Lambda_2$ if there exist a generating matrix A_1 of Λ_1 and a generating matrix A_2 of Λ_2 such that $\pi_n \circ A_1 = \pi_n \circ A_2$. Observe that if $\pi_n \circ A_1(\boldsymbol{x}) = \pi_n \circ A_2(\boldsymbol{x})$ for all $\boldsymbol{x}$ in $\boldsymbol{Z}^n$ then $\pi_n \circ A_1 = \pi_n \circ A_2$ all over $\boldsymbol{Q}^n$ hence, equality holds all over $\boldsymbol{R}^n$.

Lemma 1: Let $A = (a_{ij})$ be an $n \times n$ invertible matrix such that $\pi_n \circ A = \pi_n \circ \mathrm{I}_n$. Then $A = DP$ where D is diagonal with determinant 1 and P is a matrix of permutation.

Proof: The mapping

$$f_i: (x_1, \cdots, x_n) \mapsto \sum_{i=1}^{n} a_{ij}x_j$$

defines a linear form the kernel of which is an hyperplane denoted by H_i. If $\boldsymbol{x} \in H_i$, then $\pi_n \circ A(\boldsymbol{x}) = 0 = \pi_n(\boldsymbol{x})$ hence

$$H_i \subset \bigcup_{j=1}^{n} P_j$$

where P_j is the jth coordinate hyperplane $x_j = 0$. Therefore, H_i is equal to one of the P_j, hence $f_i = \lambda_i x_j$. Defining $\tau: i \mapsto j$ such that $f_i = \lambda_i x_{\tau(i)}$, we have

$$\prod_{i=1}^{n} \lambda_i x_{\tau(i)} = \prod_{i=1}^{n} x_i$$

hence τ is a permutation of $\{1, \cdots, n\}$ and

$$\prod_{i=1}^{n} \lambda_i = 1. \qquad \blacksquare$$

Proposition 6: Two equivalent lattices Λ_1 and Λ_2 have the same performance over the Rayleigh fading channel at high SNR.

Proof: Since Λ_1 and Λ_2 are equivalent, there exist a generating matrix A_1 of Λ_1 and a generating matrix A_2 of Λ_2 such that $\pi_n \circ A_1 = \pi_n \circ A_2$, hence $\pi_n \circ (A_1 A_2^{-1}) = \pi_n \circ \mathrm{I}_n$. From the lemma above, $A_1 = DPA_2$ where D is diagonal with determinant 1 and P is the matrix of some permutation. Therefore, the pairwise error probability functions of Λ_1 and Λ_2 have the same distribution and $\det \Lambda_1 = \det \Lambda_2$. $\blacksquare$

It is, therefore, natural to consider lattices up to equivalence.

B. Examples

Let $\Lambda_{\mathcal{O}}$ be the embedding of the number ring $\mathcal{O}$ of some totally real number field. Since we wish to improve the properties of $\Lambda_{\mathcal{O}}$ on the Gaussian channel, we need to determine the densest lattices with respect to the Euclidean distance inside the set $\mathcal{E}$ of the lattices equivalent to $\Lambda_{\mathcal{O}}$. The ratio

$$\gamma_2(\Lambda) = d_{\min}^2(\Lambda) / \det(\Lambda)^{2/n}$$

can be used to evaluate the sphere packing density of a lattice Λ. We have

Proposition 7: The sphere packing density of $\Lambda \in \mathcal{E}$ is lower-bounded by $\gamma_2(\Lambda_{\mathcal{O}})$. This statement may be rephrased as: the lattice $\Lambda_{\mathcal{O}}$ has the lowest sphere packing density inside $\mathcal{E}$.

Proof: Since $\Lambda \in \mathcal{E}$, the two lattices Λ and $\Lambda_{\mathcal{O}}$ have the same fundamental volume. Besides, any S_r-admissible lattice in $\boldsymbol{R}^n$ is such that $d^2_{\min}(\Lambda)$ is greater than the minimal distance between the origin and the boundary of S_r, i.e.,

$$d^2_{\min}(\Lambda) \geq n = d^2_{\min}(\Lambda_{\mathcal{O}}). \qquad \blacksquare$$

Let G be a generating matrix of $\Lambda_{\mathcal{O}}, \boldsymbol{\lambda} = (\lambda_1, \cdots, \lambda_n)$ and $D_{\boldsymbol{\lambda}}$ denote the diagonal matrix $\mathrm{diag}\,(\lambda_1, \cdots, \lambda_n)$. Using Lemma 1 and Proposition 7, we ought to find $\boldsymbol{\lambda}$ such that i) $\Pi_{i=1}^n \lambda_i = 1$ and ii) $d^2_{\min}(D_{\boldsymbol{\lambda}} G \boldsymbol{Z}^n)$ is as large as possible.

We propose three examples to illustrate the method.

- The ring of algebraic integers of $\boldsymbol{Q}[\sqrt{2}]$ is $\mathcal{O}_{\sqrt{2}} = \boldsymbol{Z} \oplus \sqrt{2}\boldsymbol{Z}$ and the embedding of $\boldsymbol{Q}[\sqrt{2}]$ in $\boldsymbol{R}^2$ is

$$\sigma: (a + b\sqrt{2}) \mapsto (a + b\sqrt{2}, a - b\sqrt{2}).$$

Hence, the lattice $\Lambda_{\mathcal{O}_{\sqrt{2}}}$ is generated by $\sigma(1)$ and $\sigma(\sqrt{2})$, i.e.,

$$\Lambda_{\mathcal{O}_{\sqrt{2}}} = G\boldsymbol{Z}^2 \quad \text{with} \quad G = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}.$$

Fig. 3 shows $\Lambda_{\mathcal{O}_{\sqrt{2}}}$ and the effect of the multiplication by $D_{\boldsymbol{\lambda}} = \mathrm{diag}\,(\lambda, 1/\lambda)$ on the lattice points: the points are moved along the curves $x \times y = c$. The maximum of the sphere packing density is $\gamma_{2,\max} = 1$ instead of $\gamma_2(\Lambda_{\mathcal{O}_{\sqrt{2}}}) = 1/\sqrt{2}$. It is obtained for

$$\lambda \in \{(1 + \sqrt{2})^{n+1/2}, n \in \boldsymbol{Z}\}.$$

These values yield two lattices congruent to $\boldsymbol{Z}^2$ (see Fig. 3(a)). More explicitely, we have

$$(\boldsymbol{Z}^2)_2 = U_2 \boldsymbol{Z}^2$$

where

$$U_2 = 2^{3/4} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \quad \text{and} \quad \alpha = \pm\frac{\pi}{8}.$$

The subscript indicates that these lattices offer a second-order diversity on the Rayleigh fading channel. It has been previously observed by Boullé in [3] that $\boldsymbol{Z}^2$ should be rotated by $\pi/8$ in order to get full diversity.

The periodic behavior of the curve $\gamma_2(D_{\boldsymbol{\lambda}} \Lambda_{\mathcal{O}_{\sqrt{2}}}) = f(\boldsymbol{\lambda})$ shown on Fig. 4 originates from the structure of the multiplicative group of units in a number ring. This results from the Dirichlet's unit theorem [11] which describes the organization of the lattice points on the curve $x \times y = c$. In spite of its interest, we do not give this result in order not to obscure this paper with mathematics.

- The case of the ring of algebraic integers of $\boldsymbol{Q}[\sqrt{3}]$ is similar in principle. The number ring of $\boldsymbol{Q}[\sqrt{3}]$ is $\mathcal{O}_{\sqrt{3}} = \boldsymbol{Z} \oplus \sqrt{3}\boldsymbol{Z}$ and its embedding in $\boldsymbol{R}^2$ is

$$\sigma: (a + b\sqrt{3}) \mapsto (a + b\sqrt{3}, a - b\sqrt{3}).$$

Hence, the lattice $\Lambda_{\mathcal{O}_{\sqrt{3}}}$ is generated by $\sigma(1)$ and $\sigma(\sqrt{3})$, i.e.,

$$\Lambda_{\mathcal{O}_{\sqrt{3}}} = G\boldsymbol{Z}^2 \quad \text{with} \quad G = \begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix}.$$

Fig. 4 shows the effect of the multiplication by $D_{\boldsymbol{\lambda}}$ on the lattice density. The maximum of the sphere packing density is $\gamma_{2,\max} = 2/\sqrt{3}$, instead of $\gamma_2(\Lambda_{\mathcal{O}_{\sqrt{3}}}) = 1/\sqrt{3}$. It is obtained for $\lambda \in \{(2 + \sqrt{3})^{n+1/2}, n \in \boldsymbol{Z}\}$. There is only one corresponding lattice $A_{2,2}$ which is congruent to the hexagonal lattice A_2 (see Fig. 3(b)). Specifically, we have

$$A_{2,2} = UA_2$$

where

$$U = (2\sqrt{3})^{1/2} \begin{pmatrix} \cos\left(\frac{\pi}{12}\right) & -\sin\left(\frac{\pi}{12}\right) \\ \sin\left(\frac{\pi}{12}\right) & \cos\left(\frac{\pi}{12}\right) \end{pmatrix}.$$

- Finally, we show how a rotated version of the Schläfli lattice D_4 can be found by this way with the ring of algebraic integers of $\boldsymbol{Q}[\theta], \theta = \sqrt{2 + \sqrt{2}}$. In that case, $\mathcal{O} = \boldsymbol{Z} \oplus \theta\boldsymbol{Z} \oplus \theta^2\boldsymbol{Z} \oplus \theta^3\boldsymbol{Z}$ and the lattice $\Lambda_{\mathcal{O}}$ is generated by

$$G = \begin{pmatrix} 1 & \theta & \theta^2 & \theta^3 \\ 1 & \theta' & \theta'^2 & \theta'^3 \\ 1 & -\theta & \theta^2 & -\theta^3 \\ 1 & -\theta' & \theta'^2 & -\theta'^3 \end{pmatrix}$$

where $\theta' = \sqrt{2 - \sqrt{2}}$. The effect of the multiplication by $D_{\boldsymbol{\lambda}}$ on the lattices points is again periodic. The maximum of the sphere packing density is $\gamma_{2,\max} = \sqrt{2}$, instead of $\gamma_2(\Lambda_{\mathcal{O}}) = 1/2^{3/4}$. For example, it is obtained with $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ where $\lambda_i = \sqrt{2^{-3/4}\alpha_i}$ and

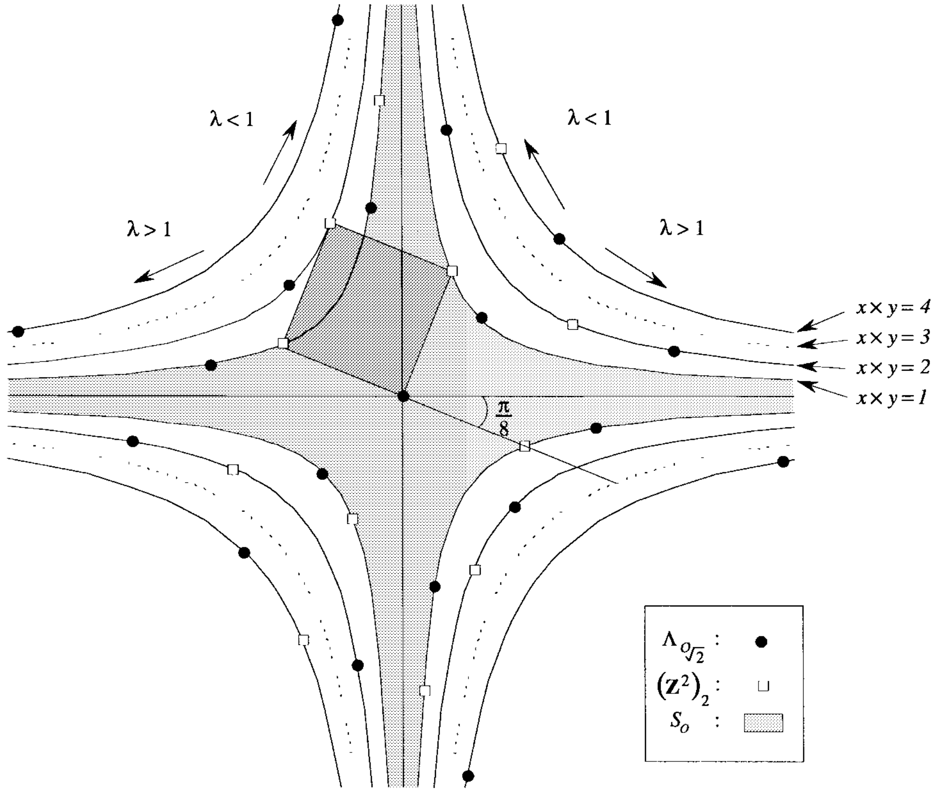
$$\begin{aligned} \alpha_1 &= (2 - \sqrt{2})(2 - \sqrt{2 - \sqrt{2}}) \\ \alpha_2 &= (2 + \sqrt{2})(2 + \sqrt{2 + \sqrt{2}}) \\ \alpha_3 &= (2 - \sqrt{2})(2 + \sqrt{2 - \sqrt{2}}) \\ \alpha_4 &= (2 + \sqrt{2})(2 - \sqrt{2 + \sqrt{2}}). \end{aligned}$$

This 4-tuple yields $D_{4,4}$, a lattice congruent to the Schläfli lattice D_4, with a fourth-order diversity on the Rayleigh fading channel. We have $D_{4,4} = D_{\boldsymbol{\lambda}} \Lambda_{\mathcal{O}} = U_4 D_4$ where U_4 is a similitude. Numerically,

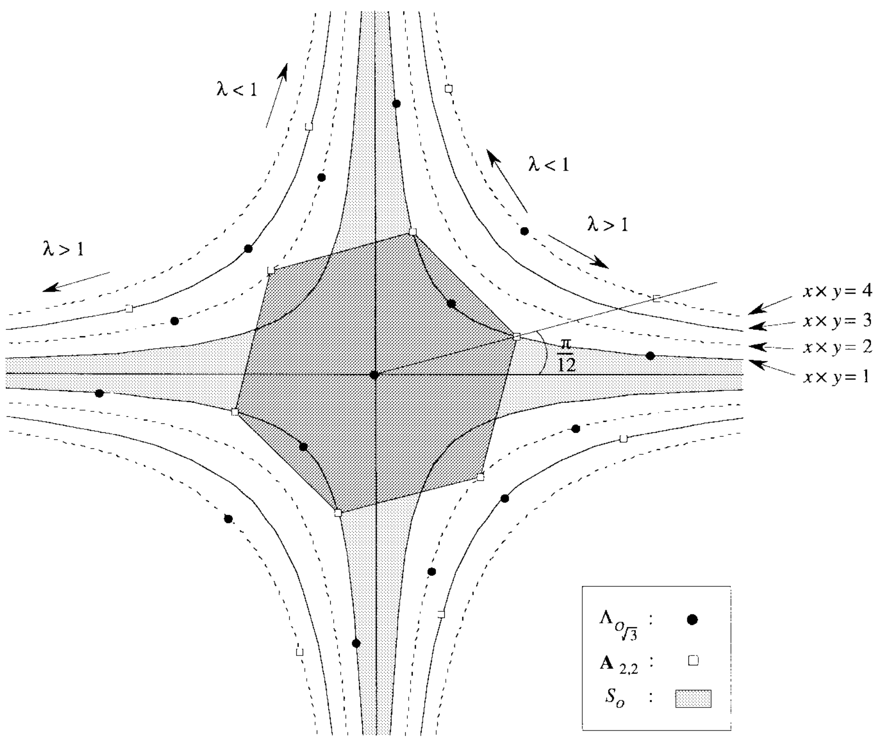
$$U_4 = \begin{pmatrix} a & b & c & d \\ -b & -c & -d & a \\ -c & -d & a & b \\ -d & a & b & c \end{pmatrix}, \quad \text{where} \begin{cases} a = -3.02516 \\ b = -2.5646 \\ c = 0.60174 \\ d = -1.71361. \end{cases}$$

The error curves obtained with constellations carved out of $(\boldsymbol{Z}^2)_2$ and $(\boldsymbol{Z}^4)_4$ for a normalized rate of 2 bits/dim are shown on Fig. 5(a) and (b). In Section VII, we shall combine these constellations with coset codes. We conjecture that the standard embedding of the ring of algebraic integers of $\boldsymbol{Q}[\theta]$ with

$$\theta = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$$



(a)



(b)

Fig. 3. (a) $\Lambda_{\mathcal{O}_{\sqrt{2}}}$ and the effect of the multiplication by $D_{\boldsymbol{\lambda}}$. (b) $\Lambda_{\mathcal{O}_{\sqrt{3}}}$ and the effect of the multiplication by $D_{\boldsymbol{\lambda}}$.

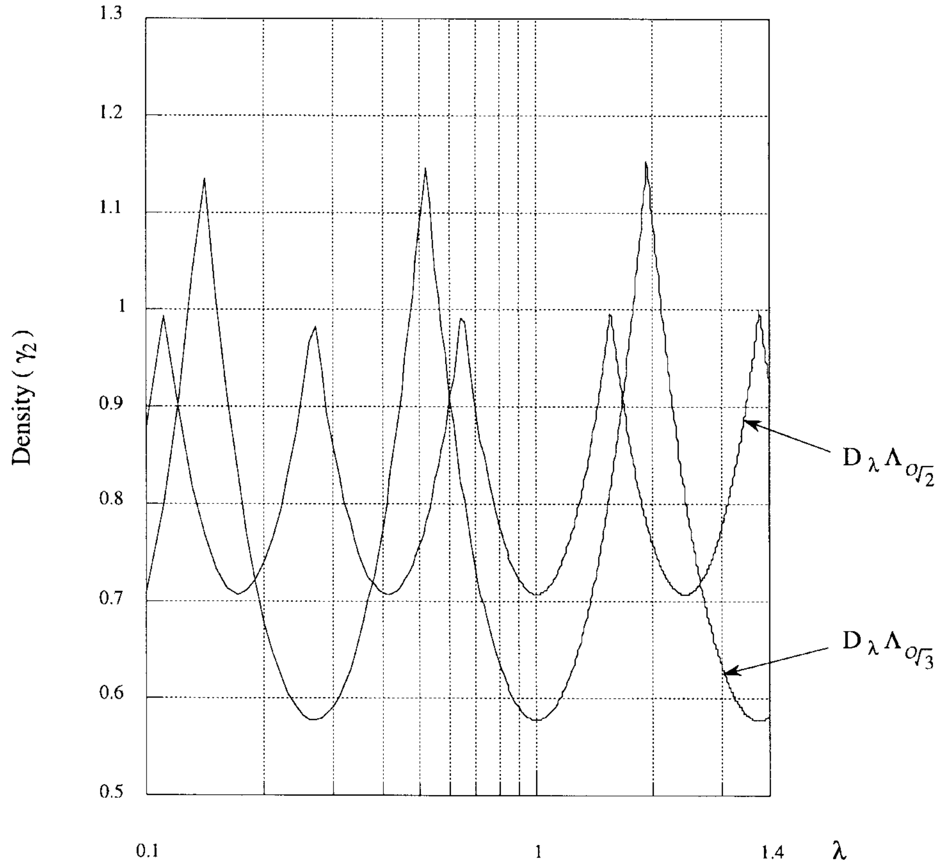


Fig. 4. $\gamma_2(D_{\boldsymbol{\lambda}}\Lambda_{\mathcal{O}_{\sqrt{2}}})$ and $\gamma_2(D_{\boldsymbol{\lambda}}\Lambda_{\mathcal{O}_{\sqrt{3}}})$ as a function of λ.

can be used to find a congruent lattice of $\boldsymbol{Z}^8$ with an eighth-order diversity and that this can be generalized with

$$\theta = \sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}.$$

VI. Of S_c-Admissible Lattice

A. Desirable Features

Recently, Boutros *et al.* have pointed out that the method proposed by Craig [13] can be further applied to construct the densest binary lattices. This method yields n-dimensional lattices with built-in diversity of order $n/2$ and good distance properties. In the remainder of the paper, we propose a simpler construction from which the Barnes–Wall lattices and the ternary lattices as defined by Forney [5], [6] can be built. The principal purpose of this section is to obtain a unitary matrix that rotates $\boldsymbol{Z}^n$ into a lattice with an $n/2$th-order diversity on the Rayleigh fading channel.

For example, the Barnes–Wall lattices are a sub-$\boldsymbol{Z}[i]$-module of the n-fold Cartesian product $\boldsymbol{Z}[i]^n$. Geometrically, their metric properties are obtained by endowing $\boldsymbol{C}^n$ with its canonical Hermitian structure

$$\forall(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{C}^n \times \boldsymbol{C}^n \quad (\boldsymbol{x}|\boldsymbol{y}) = \sum_{i=1}^{n} x_i\overline{y}_i.$$

The Cartesian product $\boldsymbol{Z}[i]^n$ can be rewritten as an orthogonal direct sum

$$\boldsymbol{Z}[i]^n = \boldsymbol{Z}[i] \oplus \boldsymbol{Z}[i] \oplus \cdots \oplus \boldsymbol{Z}[i]. \tag{5}$$

We have already noticed that the number ring $\mathcal{O}$ of an n-dimensional extension L of $\boldsymbol{Q}[i]$ is a free module of rank n over $\boldsymbol{Z}[i]$ (see Proposition 5), i.e., there exist $\mu_1,\cdots,\mu_n$ in $\mathcal{O}$ such that $\mathcal{O}$ arises as the direct sum

$$\mathcal{O} = \boldsymbol{Z}[i]\mu_1 \oplus \cdots \oplus \boldsymbol{Z}[i]\mu_n$$

hence its embedding in $\boldsymbol{C}^n$ is

$$\Lambda_{\mathcal{O}} = \boldsymbol{Z}[i]\sigma(\mu_1) \oplus \cdots \oplus \boldsymbol{Z}[i]\sigma(\mu_n). \tag{6}$$

Both (5) and (6) are formally very similar and one may wonder what is preventing $\Lambda_{\mathcal{O}}$ from having a sub-$\boldsymbol{Z}[i]$ module congruent to the n-dimensional Barnes–Wall lattice. Observe that the sum (5) is an orthogonal direct sum whereas it is only direct in (6). If the family $(\sigma(\mu_1),\cdots,\sigma(\mu_n))$ can be made orthonormal with respect to the canonical Hermitian structure of $\boldsymbol{C}^n$ then $\boldsymbol{Z}[i]^n$ and $\Lambda_{\mathcal{O}}$ are congruent; we shall say that the embedding σ is isometric. In that case, there is a similarity, the matrix of which is denoted by A, such that $\Lambda_{\mathcal{O}} = A\boldsymbol{Z}[i]^n$. Besides, if G is a generating matrix over $\boldsymbol{Z}[i]^n$ of some lattice Λ, then $A\Lambda = AG\boldsymbol{Z}[i]^n$ is a sublattice of $\Lambda_{\mathcal{O}}$ congruent to Λ. As such

- from the properties of $\Lambda_{\mathcal{O}}$, any constellation carved out of $A\Lambda$ offers an nth-order diversity.

- since $A\Lambda$ and Λ are congruent, they have the same properties over the Gaussian channel.

B. The Construction

We now look for a sufficient condition for the embedding σ to be isometric. The following lemma recalls simple properties of polynomials which will prove useful in the following.

Lemma 2: Let $\alpha_1, \cdots, \alpha_n$ be the roots over $\boldsymbol{C}$ of $P(X) = X^n - a$ where $a \in \boldsymbol{C}$ and $|a| = 1$. Then

$$S_p = \sum_{k=1}^{n} \alpha_k^p = 0, \quad \text{if } 1 \le k \le n-1 \tag{7}$$

$$S = \sum_{k=1}^{n} |\alpha_k|^2 = n. \tag{8}$$

Proof: This fact stems from the properties of the nth roots of unity in $\boldsymbol{C}$, specifically

$$\sum_{k=0}^{n-1} (\omega^p)^k = 0$$

where $\omega = \exp(2i\pi/n)$ and $1 \le p \le n-1$. ■

The cyclotomic fields exert a great deal of control over algebraic number theory in general. For example, when transmission occurs on a Rayleigh fading channel, the decoding of a constellation carved out of a lattice Λ can be eased if Λ has a circulant generating matrix [2]. In fact, it is a theorem that for $\Lambda_{\mathcal{O}}$ to have a circulant generating matrix, the number field L needs to be contained in a cyclotomic field. Let θ_N be a Nth primitive root of unity. The field $\boldsymbol{Q}[\theta_N]$ is called a cyclotomic extension of order N. The dimension of a cyclotomic extension over $\boldsymbol{Q}$ is related to the Euler function φ which assigns to each positive integer n the number $\varphi(N)$ of integers k such that $1 \le k \le N$ and $k \wedge n = 1$. For example, for every prime p, we have $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ and if p and q are relatively prime, then $\varphi(p \times q) = \varphi(p) \times \varphi(q)$. Finally, the number ring of $\boldsymbol{Q}[\theta_N]$ over $\boldsymbol{Q}$ is $\boldsymbol{Z}[\theta_N]$. Two situations are of special interest,

- *Situation 1:* If $N = 2^r\,(r \ge 3)$ then $\boldsymbol{Q}[i]$ is contained in $\boldsymbol{Q}[\theta_N]$, specifically, the field $\boldsymbol{Q}[\theta_N]$ is an extension of order

$$n = \frac{\varphi(N)}{2} = 2^{r-2}$$

of $\boldsymbol{Q}[i]$. The number ring of $\boldsymbol{Q}[\theta_N]$ over $\boldsymbol{Q}[i]$ is $\mathcal{O}_n = \boldsymbol{Z}[i][\theta_N]$. An integral basis of $\mathcal{O}_n$ over $\boldsymbol{Z}[i]$ is $(1, \theta_N, \cdots, \theta_N^{n-1})$. Consequently, a generating matrix of the embedding $\Lambda_{\mathcal{O}_n}$ of $\mathcal{O}_n$ in $\boldsymbol{C}^n$ is the Vandermonde matrix

$$G_n = \mathrm{VDM}\,(\theta_{N,1}, \cdots, \theta_{N,n})$$

where $\theta_{N,1} = \theta_N, \cdots, \theta_{N,n}$ are the roots of the minimal polynomial $M_{\theta_N} = X^n - i$ of θ_N over $\boldsymbol{Q}[i]$. In short, $\Lambda_{\mathcal{O}_n} = G_n \boldsymbol{Z}[i]^n$.

- *Situation 2:* If $N = 3^2 \times 2^r\,(r \ge 1)$ then $\boldsymbol{Q}[j]$ is contained in $\boldsymbol{Q}[\theta_N]$ and $\boldsymbol{Q}[\theta_N]$ is an extension of order

$$n = \frac{\varphi(N)}{2} = 3 \times 2^{r-1}$$

of $\boldsymbol{Q}[j]$. The number ring of $\boldsymbol{Q}[\theta_N]$ over $\boldsymbol{Q}[j]$ is $\mathcal{O}_n = \boldsymbol{Z}[j][\theta_N]$. An integral basis of $\mathcal{O}_n$ is $(1, \theta_N, \cdots, \theta_N^{n-1})$ hence, a generating matrix of the embedding $\Lambda_{\mathcal{O}_n}$ of $\mathcal{O}_n$ in $\boldsymbol{C}^n$ is again the Vandermonde matrix

$$G_n = \mathrm{VDM}\,(\theta_{N,1}, \cdots, \theta_{N,n})$$

where $\theta_{N,1} = \theta_N, \cdots, \theta_{N,n-1}$ are the roots of the minimal polynomial $M_{\theta_N} = X^n + j$ of θ_N over $\boldsymbol{Q}[j]$ and we have $\Lambda_{\mathcal{O}_n} = G_n \boldsymbol{Z}[j]^n$.

Both facts can be derived from the key results gathered in section 4.1 and from the fact that if L is an extension field of K then the dimension of L as a vector space over $\boldsymbol{Q}$ is the product of the dimension of L over K by the dimension of K over $\boldsymbol{Q}$. Finally, the minimal polynomials are derived by factorizing $X^N - 1$ in $\boldsymbol{Q}[i]$ in the first case, and in $\boldsymbol{Q}[j]$ in the second instance.

Proposition 8: The matrix $(1/\sqrt{n})G_n$ is unitary.

Proof: Let $C_k = (\theta_{N,1}^{k-1}, \cdots, \theta_{N,n}^{k-1})(1 \le k \le n)$ denote the kth column of G_n. From (6), we have

$$||C_k||^2 = \sum_{i=1}^{n} |\theta_{N,i}^{k-1}|^2 = n$$

and orthogonality stems from (5)

$$(C_k|C_l) = \sum_{i=1}^{n} \theta_{N,i}^{k-1}\overline{\theta}_{N,i}^{l-1} = \sum_{i=1}^{n} \theta_{N,i}^{k-l} = 0, \quad \text{if } k \ne l \quad ■$$

Proposition 8 says that $\Lambda_{\mathcal{O}_n}$ and $\boldsymbol{Z}[i]^n$ are congruent in the first situation whereas $\Lambda_{\mathcal{O}_n}$ and $\boldsymbol{Z}[j]^n$ are congruent in the second one.

C. Examples

- *Situation 1 (cont.):* In the case of Situation 1 where $n = 2^{r-2}(r \ge 3)$, lattices congruent to the Barnes–Wall lattices and their principal sublattices can be easily obtained. If Λ_n is the Barnes–Wall lattices of dimension $2n$ or some of its sublattices, then $G_n\Lambda_n$ is a congruent version of Λ_n which offers an nth-order diversity on the Rayleigh fading channel instead of the one-order diversity of the standard version. For example, with ϕ denoting the Gaussian integer $1+i$, we have:

▹ Following [5], the lattice D_4 arises as

$$D_4 = \begin{pmatrix} 1 & 0 \\ 1 & \phi \end{pmatrix} \boldsymbol{Z}[i]^2.$$

Applying the method described in Section VI-B with $N = 8$, a congruent version of D_4 with diversity 2 on the Rayleigh fading channel is $D_{4,2} = G_2 D_4$ where

$$G_2 = \begin{pmatrix} 1 & \theta \\ 1 & -\theta \end{pmatrix}, \qquad \text{with} \quad \theta = \exp\left(i\frac{\pi}{4}\right).$$

As for D_4, the construction also naturally points to structural decomposition

$$D_{4,2} = \sigma(\phi\mathcal{O}_2 + (2,1,2))$$

where $(2,1,2)$ is the binary repetition code. With a slight modification of the trellis diagram of D_4, we can represent $D_{4,2}$ by a two section-trellis diagram (see Fig. 6(a)). It is based upon the Cartesian product of two binary partitions of $\boldsymbol{Z}[i]$ and $\theta\boldsymbol{Z}[i]$ properly embedded in $\boldsymbol{C}^2$, namely,

$$(\boldsymbol{Z}[i]/\phi\boldsymbol{Z}[i]) \times (\theta\boldsymbol{Z}[i]/\phi\theta\boldsymbol{Z}[i]).$$

▹ The lattice E_8 is obtained as

$$E_8 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & \phi & 0 & 0 \\ 1 & 0 & \phi & 0 \\ 1 & \phi & \phi & \phi^2 \end{pmatrix} \boldsymbol{Z}[i]^4$$

or as

$$E_8 = \phi^2 \boldsymbol{Z}[i]^4 + \phi(4,3,2) + (4,1,4).$$

A congruent version of E_8, denoted by $E_{8,4}$, with diversity 4 on the Rayleigh fading channel is therefore

$$E_{8,4} = \sigma(\phi^2 \mathcal{O}_4 + \phi(4,3,2) + (4,1,4)) = G_4 E_8$$

where

$$G_4 = \begin{pmatrix} 1 & \theta & \theta^2 & \theta^3 \\ 1 & -\theta & \theta^2 & -\theta^3 \\ 1 & i\theta & -\theta^2 & -i\theta^3 \\ 1 & -i\theta & -\theta^2 & i\theta^3 \end{pmatrix} \quad \text{with} \quad \theta = \exp\left(i\frac{\pi}{8}\right).$$

Again $E_{8,4}$ can be represented by a four section-trellis diagram (see Fig. 6(b)) similar to that of E_8.

These congruent versions of the Barnes–Wall lattices are based upon the Cartesian product of the following binary partitions rather than from repeated binary partition of $\boldsymbol{Z}[i]$ that would lead to a one-order diversity on the Rayleigh fading channel

$$\begin{aligned} &\boldsymbol{Z}[i]/\phi\boldsymbol{Z}[i]/\phi^2\boldsymbol{Z}[i]/\cdots \\ &\theta\boldsymbol{Z}[i]/\phi\theta\boldsymbol{Z}[i]/\phi^2\theta\boldsymbol{Z}[i]/\cdots \\ &\vdots \\ &\theta^{n-1}\boldsymbol{Z}[i]/\phi\theta^{n-1}\boldsymbol{Z}[i]/\phi^2\theta^{n-1}\boldsymbol{Z}[i]/\cdots. \end{aligned}$$

Besides, the trellis diagram of the congruent version is almost identical to the trellis of its standard counterpart as described in [5].

• *Situation 2 (cont.):* In that case $n = 3 \times 2^{r-1}$, $r \geq 1$ and $\Lambda_{\mathcal{O}_n}$ and $\boldsymbol{Z}[j]^n$ are congruent. It is known that coset code construction based upon repeated ternary partitions of the hexagonal lattice generates E_6, K_{12}, K_{24}, and Λ_{24} in particular. Congruent versions of these lattices can be obtained in the same way as before as $E_{6,3} = G_3 E_6, K_{12,6} = G_6 K_{12}, K_{24,12} = G_{12} K_{24}$, and $\Lambda_{24,12} = G_{12}\Lambda_{24}$. Each of them offers an $n/2$th-order diversity on the Rayleigh fading channel and their code formula representations still hold. For example [6], the lattice E_6 can be written as

$$E_6 = \phi\boldsymbol{Z}[j]^3 + (3,1,3) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & \phi & 0 \\ 1 & 0 & \phi \end{pmatrix} \boldsymbol{Z}[j]^3$$

where $\phi = 1 + 2j = i\sqrt{3} \in \boldsymbol{Z}[j]$ and $C = (3,1,3)$ is the ternary repetition code. Hence, $E_{6,3}$ arises as

$$E_{6,3} = \sigma(\phi\mathcal{O}_3 + (3,1,3)) = G_3 E_6$$

where

$$G_3 = \begin{pmatrix} 1 & -\theta & \theta^2 \\ 1 & -j\theta & -(1+j)\theta^2 \\ 1 & -j^2\theta & -(1+j^2)\theta^2 \end{pmatrix} \quad \text{and} \quad \theta = \exp\left(i\frac{2\pi}{9}\right).$$

Again this congruent version of E_6 can be represented by a three section-trellis diagram as shown in Fig. 6(c). Instead of being constructed from repeated ternary partition of $\boldsymbol{Z}[j]$, the lattice $E_{6,3}$ is based upon the Cartesian product of the three following ternary partitions properly embedded in $\boldsymbol{C}^3$

$$(\boldsymbol{Z}[j]/\phi\boldsymbol{Z}[j]) \times (\theta\boldsymbol{Z}[j]/\phi\theta\boldsymbol{Z}[j]) \times (\theta^2\boldsymbol{Z}[j]/\phi\theta^2\boldsymbol{Z}[j]).$$

VII. Coset Codes on Constellations Matched to the Rayleigh Fading Channel

A. The Partitioning Rules

On the Gaussian channel, a coset code, with good Euclidean distance properties relies upon a partition of the signal set with minimum distance at a given partition level as large as possible. On the Rayleigh fading channel, the situation is very different in the sense that we cannot use any norm to evaluate the separation between two symbols, but still it is similar in principle since we want to group signals into subsets with minimal component product $|x_1 \times \cdots \times x_n|$ as large as possible. Here as well, number field theory provides an appropriate tool to increase the minimal component product, while keeping the constellation expansion under control. In what follows, we shall keep the notation introduced in Section IV-B. We denote by $\mathcal{O}$ the number ring over R of some finite extension $K[\theta]$ of K of degree n. The embedding of $\mathcal{O}$ in $\boldsymbol{C}^n$ is denoted by σ and $\sigma(\mathcal{O})$ is written $\Lambda_{\mathcal{O}}$.

We work with $\mathcal{O}$ rather than with its embedding $\Lambda_{\mathcal{O}}$ for grouping the symbols, i.e., the elements of $\mathcal{O}$, into subsets with large minimal algebraic norm. We recall that the algebraic norm is multiplicative, that is, $N(xy) = N(x)N(y)$, hence, if ϕ is some algebraic integer,

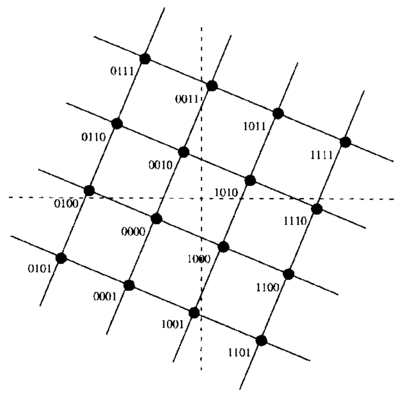
$$\min_{\substack{x \in \phi\mathcal{O} \\ x \neq 0}} |N(x)| = |N(\phi)| \min_{\substack{x \in \mathcal{O} \\ x \neq 0}} |N(x)| = |N(\phi)|.$$

Multiplication by ϕ provides an algebraic means to systematically partition $\mathcal{O}$ and guarantee a good minimal algebraic norm. Hence, we study the additive groups sandwiched between $\mathcal{O}$ and $\phi\mathcal{O}$.

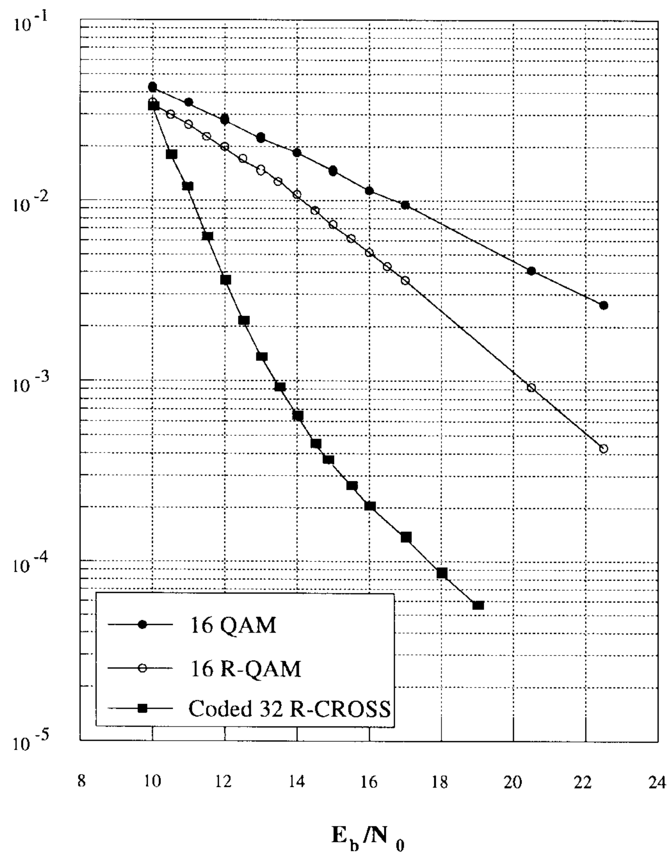
We recall that the number ring $\mathcal{O}$ is a free R-module of rank n and so is $\phi\mathcal{O}$, therefore, any R-module sandwiched between $\mathcal{O}$ and $\phi\mathcal{O}$ is a free R-module of rank n over R. Besides, if $\mu_1, \cdots, \mu_n$ is an R-basis of $\mathcal{O}$ then the $n \times n$ matrix A, the columns of which are $\sigma(\mu_1), \cdots, \sigma(\mu_n)$, generates $\Lambda_{\mathcal{O}}$, i.e., $\Lambda_{\mathcal{O}} = AR^n$ hence, $\phi\mu_1, \cdots, \phi\mu_n$ is an R-basis of $\mathcal{O}$, and a generating matrix of $\Lambda_{\phi\mathcal{O}} = \sigma(\phi\mathcal{O})$ is $D_\phi A$ where

$$D_\phi = \operatorname{diag}(\sigma_1(\phi), \cdots, \sigma_n(\phi)).$$

Since $\mathcal{O}\,/\,\phi\mathcal{O}$ and $\Lambda_{\mathcal{O}}\,/\,\Lambda_{\phi\mathcal{O}}$ are isomorphic, the index of $\phi\mathcal{O}$ in $\mathcal{O}$ is $|\det D_\phi| = |N(\phi)|$ if $R = \boldsymbol{Z}$ and it is $|\det D_\phi|^2 = |N(\phi)|^2$ if $R = \boldsymbol{Z}[i]$ or $R = \boldsymbol{Z}[j]$. For example, if $|N(\phi)| = 2$ and $R = \boldsymbol{Z}$ then the partition is two way.



16 R-QAM carved out $(\mathbf{Z}^2)_2$



(a)

Fig. 5. Bit-error rate on the Rayleigh fading channel (spectral efficiency: $\rho = 2$). (a) $\boldsymbol{Z}^2$-type constellations.

Finally, let I be some index set. An additive group sandwiched between $\mathcal{O}^I$ and $\phi\mathcal{O}^I$ can be represented by means of the code formula

$$M = C + \phi\mathcal{O}^I$$

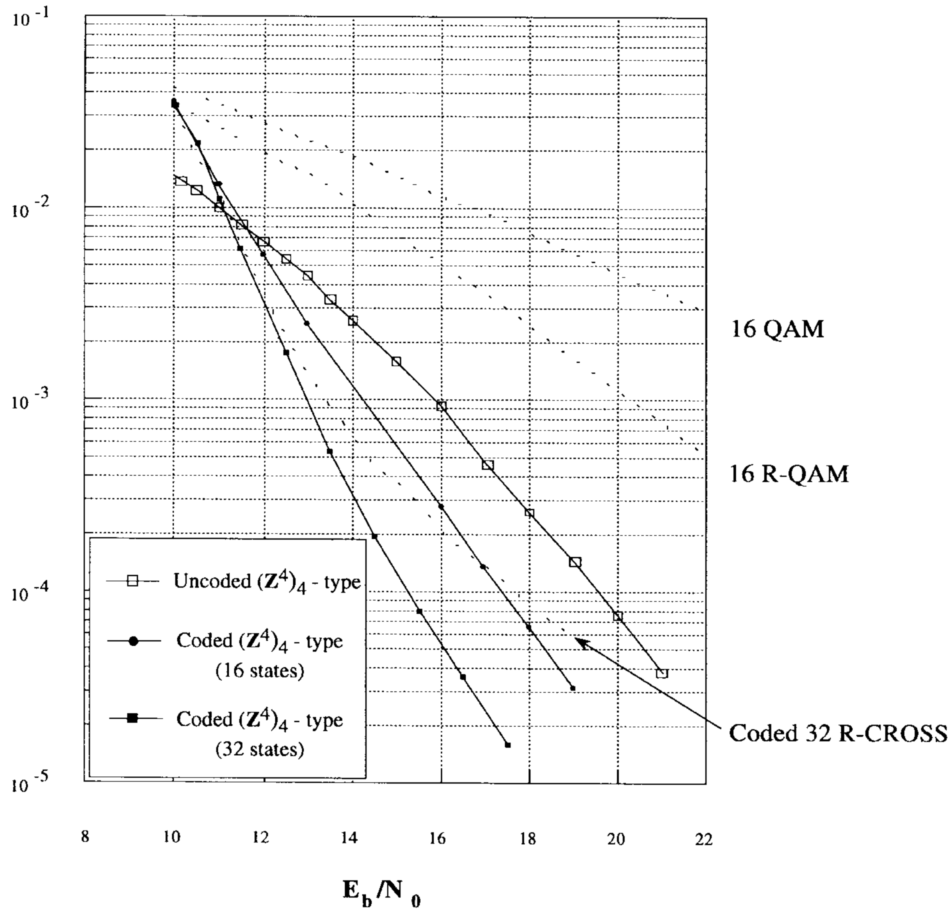
where C is a subgroup of $(\mathcal{O}/\phi\mathcal{O})^I$, i.e., a code over $\mathcal{O}/\phi\mathcal{O}$. Nevertheless, all the sets obtained in this way are not necessarily R-modules.

As far as its effect on the Euclidean distance is concerned, the multiplication by $\phi \in \mathcal{O}$ in a number field is not easily analyzed in general because the algebraic norm and the Euclidean distance cannot be related. Nonetheless, when ϕ is chosen in $R, \Lambda_{\mathcal{O}}$ and $\sigma(\phi\mathcal{O})$ are congruent and we have

$$\min_{\substack{x \in \Lambda_{\phi\mathcal{O}} \\ x \neq 0}} ||x||_2^2 = |\phi|^2 \times \min_{\substack{x \in \Lambda_{\mathcal{O}} \\ x \neq 0}} ||x||_2^2. \tag{9}$$

B. The Coding Gain on the Rayleigh Fading Channel

The coding gain is determined by the coder and the subset partitioning. A simple expression for the gain has been obtained on the Gaussian channel [5] and we look for a similar expression on the Rayleigh channel in this section. For this purpose, we define the following three parameters:



(b)

Fig. 5. *(Continued.)* Bit-error rate on the Rayleigh fading channel (spectral efficiency: $\rho = 2$). (b) $\boldsymbol{Z}^4$-type constellations.

- *The partitioning gain:*

$$g_p = |N(\phi)|^{2/n}. \qquad (10)$$

- *The diversity gain:*

At high SNR, we recall that the pairwise error probability simplifies as given in (2)

$$p(\boldsymbol{x} \to \boldsymbol{y}) \leq \prod_{x_i \neq x_j} \frac{1}{K|x_i - y_i|^2} = \prod_{i=1}^{n} \frac{1}{K|x_i - y_i|^2}$$

because the coordinates of two different channel symbols picked in $\Lambda_{\mathcal{O}}$ are all distinct. Hence, if $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_p$ and $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_p$ are two symbol sequences then

$$p((\boldsymbol{x}_k) \to (\boldsymbol{y}_k)) \leq \prod_{\boldsymbol{x}_k \neq \boldsymbol{y}_k} p(\boldsymbol{x}_k \to \boldsymbol{y}_k).$$

The Hamming weight of $\boldsymbol{c} \in (\mathcal{O}/\phi\mathcal{O})^I$ is the cardinality of the support of $\boldsymbol{c}$. We denote by $d_H(C)$ the minimal Hamming distance of the code C. The diversity gain arises from the fact that when an incorrect path is selected, the number of erroneous symbols is equal or greater than the minimal Hamming distance of the code, whereas in the uncoded case, there may be a single erroneous symbol only. In other words, if $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_p$ and $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_p$ are nonparallel, they differ on at least $d_H(C)$ positions. Hence

$$p((\boldsymbol{x}_k) \to (\boldsymbol{y}_k)) \leq \frac{1}{(K^n N_0^2)^{d_H(C)}}$$

where

$$N_0 = \min_{\substack{x \in \mathcal{O} \\ x \neq 0}} N(x).$$

For the uncoded constellation

$$p((\boldsymbol{x}_k) \to (\boldsymbol{y}_k)) \leq \frac{1}{K^n N_0^2}.$$

Besides $N_0 = 1$, therefore, the gain is

$$g_D(C) \geq \left[\frac{(K^n)^{d_H(C)}}{K^n}\right]^{1/n} = K^{d_H(C)-1}. \qquad (11)$$

Observe that the minimal algebraic norm may not be increased when an incorrect path is selected, but the diversity order is certainly increased.

- *The expansion factor:*

For brevity, we restrict ourselves to the case of convolutional codes for which $I = \boldsymbol{Z}$. The expansion factor is defined by [5] as

$$e_f = \left|\frac{\det(\Lambda^0)}{\det(\Lambda_{\mathcal{O},r})}\right|^{2/nv} \qquad (12)$$

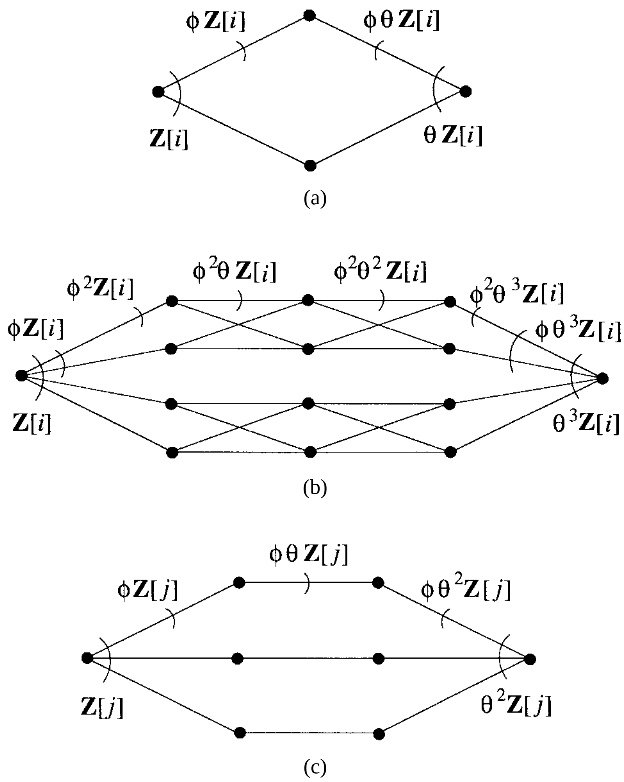


Fig. 6. Trellis diagram of (a) $D_{4,2}$, (b) $E_{8,4}$, and (c) $E_{6,3}$.

where Λ^0 is the input lattice, $v = 1$ if $R = \boldsymbol{Z}$ and $v = 2$ if $R = \boldsymbol{Z}[i]$ or $R = \boldsymbol{Z}[j]$. The number

$$\left| \frac{\det(\Lambda^0)}{\det(\Lambda_{\mathcal{O},r})} \right|$$

is the index of Λ^0 in the lattice $\Lambda_{\mathcal{O},r}$.

The fundamental coding gain is

$$\gamma_R = \frac{\min(g_p, g_D(C))}{e_f}. \tag{13}$$

It depends on the signal-to-noise ratio through g_D; nonetheless, when the signal-to-noise ratio increases and $d_H(C) \geq 2$, then the gain tends toward

$$\gamma_{R,\infty} = \frac{g_p}{e_f}. \tag{14}$$

This parameter no longer depends on $d_H(C)$. Since we wish to guarantee $d_H(C) \geq 2$ in order to reach the partitioning gain, we need TCM codes whose parallel transition group is $\phi\mathcal{O}$. If $d_H(C)$ is increased, the partitioning gain is reached with smaller values of the signal-to-noise ratio. Hence, there is a tradeoff between the complexity and the speed for obtaining the partitioning gain. The gains are valid for large signal sets and do not take into account side effects due to the mapping at the bit level.

C. Examples

In order to propose an easily implementable construction, we look for an algebraic integer $\phi \in \mathcal{O}$ such that $N(\phi) = 2$. Two coset codes already used on the Gaussian channel with $\boldsymbol{Z}^2$-type and $\boldsymbol{Z}^4$-type signal sets, respectively, are combined with the lattice constellations built in Section V-B where $R = \boldsymbol{Z}$ and $v = 1$. These two schemes display good performance on both the fading channel and the Gaussian channel. Computer simulations confirm our theoretical analysis.

• *Example 1:* A 32-CROSS signal set rotated by $\pi/8$ is combined with a 64-state Ungerboeck code of rate $2/3$ [15]. The partition chain with the corresponding minimum distances and the minimum algebraic norms are shown below. This partition corresponds to the multiplication by $\phi = \sqrt{2}$ in $\mathcal{O} = \boldsymbol{Z}[\sqrt{2}]$.

$\phi = \sqrt{2}$		$\lvert N(\phi)\rvert = 2$	$d^2_{\min}$	Minimal alg. norm
$\mathcal{O} = \boldsymbol{Z}[\phi]$	$\xrightarrow{D_\lambda \circ \sigma}$	$(\boldsymbol{Z}^2)_2$	1	1
$\phi\mathcal{O}$		$(\Re\boldsymbol{Z}^2)_2$	2	2
$2\mathcal{O}$		$2(\boldsymbol{Z}^2)_2$	4	4

It is optimal in the sense that $\phi\mathcal{O}$ is embedded onto the lattice $U_2\Re\boldsymbol{Z}^2$. Therefore, the minimum Euclidean norm and the minimum algebraic norm are multiplied by two at each partition level. Consequently, the fundamental coding gain is $\gamma_G = 3.5$ (5.44 dB) on the Gaussian channel, whereas the asymptotic gain on the Rayleigh fading channel is $\gamma_{R,\infty} = 4$ (6 dB). Simulations results are shown in Fig. 5(a). The uncoded 16-QAM rotated by $\pi/8$ is denoted by 16-R-QAM and the coded 32-CROSS rotated by $\pi/8$ is referred to as a coded 32-R-CROSS.

• *Example 2:* The four-dimensional trellis modulation scheme described in this subsection employ a compact set of 2^9 points picked out of $(\boldsymbol{Z}^4)_4 = U_4\boldsymbol{Z}^4$. The partition

$$D_4/\Re\boldsymbol{Z}^4/\Re D_4/2\boldsymbol{Z}^4$$

is mapped by U_4 on the partition obtained when $D_{\boldsymbol{\lambda}} \circ \sigma$ is applied to

$$\boldsymbol{Z}[\phi]/\phi\mathcal{O}/\phi^2\mathcal{O}/\phi^3\mathcal{O}$$

where

$$\phi = \sqrt{2 + \sqrt{2}}$$

as shown below. The minimum algebraic norm is multiplied by two at each partition level and the minimum Euclidean distances are

$$d_0^2/2d_0^2/2d_0^2/4d_0^2/4d_0^2/8d_0^2/\cdots$$

where d_0 is the minimum Euclidean distance of $(\boldsymbol{Z}^4)_4$.

			$d^2_{\min}$	Minimal alg. norm
$\phi = \sqrt{2+\sqrt{2}}$		$\lvert N(\phi)\rvert = 2$		
		$(\boldsymbol{Z}^4)_4$	1	$\frac{1}{2}$
$\mathcal{O} = \boldsymbol{Z}[\phi]$	$\xrightarrow{D_\lambda \circ \sigma}$	$D_{4,4}$	2	1
$\phi\mathcal{O}$		$(\Re \boldsymbol{Z}^4)_4$	2	2
$\phi^2\mathcal{O}$		$(\Re D_4)_4$	4	4
$\phi^3\mathcal{O}$		$2(\boldsymbol{Z}^4)_4$	4	8
$2\mathcal{O}$		$2D_{4,4}$	8	16

Hence we have partitioned $\boldsymbol{Z}^4$ as proposed by [15], [16] in order to build 16 subsets of type $\boldsymbol{Z}^4$ with 32 points each. Next we rotate them by applying U_4. The constellation is combined with a 16-state Wei code of rate $2/3$ and with a 32-state Ungerboeck code of rate $3/4$. In the latter case, the fundamental gains have the same value on the Gaussian channel and on the Rayleigh fading channel, $\gamma_G = \gamma_{R\infty} = 2^{3/2}$ (4. 52 dB) whereas in the first case, $\gamma_G = 2^{3/2}$ and $\gamma_{R\infty} = 2$. On the Gaussian channel, the number of states is increased in order to minimize the error coefficient and the corresponding improvement is small. On the contrary, there is always a significant advantage in increasing the partition depth on the Rayleigh fading channel.

A similar partition can be obtained with the lattice $D_{4,2}$ built in Section VI-C, Situation 1. Indeed, since $\phi = 1 + i \in R = \boldsymbol{Z}[i]$, the situation is much simpler because multiplication by ϕ is easily analyzed with respect to

- its effect on the minimal Euclidean distance, it is multiplied by 2 at each partition level;
- its effect on the minimal algebraic norm, it is multiplied by $|N(\phi)| = 2$ at each partition level.

We keep the notation introduced in Section VI–C, we recall that $\theta = \exp(i(\pi/4))$. We have

			$d^2_{\min}$	Minimal alg. norm
$\phi = 1+i$		$\lvert N(\phi)\rvert = 2$		
$\mathcal{O} = \boldsymbol{Z}[i][\theta]$	$\xrightarrow{\sigma}$	$(\boldsymbol{Z}^4)_2$	1	1
$\phi\mathcal{O}$		$(\Re \boldsymbol{Z}^4)_2$	2	2
$2\mathcal{O}$		$2(\boldsymbol{Z}^4)_2$	4	4

What makes the previous situation preferable is the diversity order four, instead of two in this case.

VIII. Conclusion

We have built lattice constellations for the fading channel in such a way as to embrace all the good known constellations and to suggest extensions. Coset codes combined with such constellations are characterized in a similar way as on the Gaussian channel in terms of geometrical parameters such as the fundamental coding gain.

A good partition is obtained when the natural partition of the number ring from which the constellation originates is mapped onto a good partition with respect to the Euclidean distance. When the partition is congruent to the partition of a binary lattice, Ungerboeck's codes or Wei's codes offer significant gain on the Rayleigh fading channel with unchanged performance on the Gaussian channel.

On the decoding side, two- and four-dimensional schemes do not require highly efficient algorithms and the suboptimum decoder proposed by Boutillon [17] has proved good enough. However, since the achievable diversity order increases with the dimension, the need for an efficient decoding algorithm is obvious.

References

[1] X. Giraud and J. C. Belfiore, "Constellations matched to the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 42, pp. 106–115, Jan. 1996.

[2] X. Giraud, "Constellations matched to the fading channels," Ph.D. dissertation, ENST, Paris, France, May 1994.

[3] K. Boullé and J. C. Belfiore, "Modulation schemes designed for the Rayleigh fading channel," presented at CISS'92, Princeton, NJ, Mar. 1992.

[4] G. D. Forney Jr. "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sept. 1991.

[5] ——, "Coset codes—Part I and Part II," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123–1187, Jan. 1988.

[6] ——, "Ternary codes, lattices and trellis codes," unpublished.

[7] P. M. Grüber and C. G. Lekkerkerker, *Geometry of Numbers*. Amsterdam, The Netherlands: North-Holland Math. Library Elsevier, 1987.

[8] D. Divsalar and M. K. Simon, "The design of trellis coded MPSK for fading channels: Performance criteria," *IEEE Trans. Commun.*, vol. 36, pp. 1004–1012, Sept. 1988.

[9] J. A. Rush, "Constructive packing of crosspolytopes," *Mathematika*, vol. 38, pp. 376–380, 1991.

[10] M. Siala, X. Giraud, and G. K. Kaleh, "Lee metric coset codes and their performance on some Rician channels," in *Proc. Int. Conf. on Telecommunications* (Istanbul, Turkey, Apr. 1996).

[11] D. A. Marcus, *Number Fields* (University Texts). New York: Springer-Verlag, 1977.

[12] S. Lang, *Algebraic Number Fields* (Graduate Texts in Mathematics). New York: Springer-Verlag, 1986.

[13] M. Craig, "Extreme forms and cyclotomy," *Mathematika*, vol. 25, pp. 236–241, 1978.

[14] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, "Good lattice constellations for both Rayleigh and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, pp. 502–518, Mar. 1996.

[15] G. Ungerboeck, "Trellis-coded modulation with redundant signal sets, Part II," *IEEE Commun. Mag.*, vol. 25, no. 2, Feb. 1987.

[16] L. F. Wei, "Trellis-coded modulations with multidimensional constellations," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 483–501, July 1987.

[17] E. Boutillon, "A VLSI architecture of a decoder for TCM using admissible lattices designed for the Rayleigh fading channel," presented at ICC'94, New Orleans, LA.