Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels

Joseph Boutros, Emanuele Viterbo, Catherine Rastello, and Jean-Claude Belfiore, *Member, IEEE*

Abstract— **Recent work on lattices matched to the Rayleigh fading channel has shown how to construct good signal constellations with high spectral efficiency. In this paper we present a new family of lattice constellations, based on complex algebraic number fields, which have good performance on Rayleigh fading channels. Some of these lattices also present a reasonable packing density and thus may be used at the same time over a Gaussian channel. Conversely, we show that particular versions of the best lattice packings (D_4, E_6, E_8, $K_{12}, \Lambda_{16}, \Lambda_{24}$), constructed from totally complex algebraic cyclotomic fields, present better performance over the Rayleigh fading channel. The practical interest in such signal constellations rises from the need to transmit information at high rates over both terrestrial and satellite links.**

Index Terms— **Lattices, number fields, fading channels, code diversity.**

This paper is dedicated to the memory of Catherine Rastello who left us in April 1995.

I. Introduction

THE interest in trellis-coded modulation (TCM) for fading channels dates back to 1988, when Divsalar and Simon [1] fixed design rules and performance evaluation criteria. Following the ideas in [1], Schlegel and Costello [2] found new 8-PSK trellis codes for the Rayleigh channel. These codes exhibit higher diversity than Ungerboeck's 8-PSK codes, only when the trellis exceeds 64 states.

An alternative method to gain diversity is the use of multidimensional 8-PSK trellis codes proposed by Pietrobon *et al.* [3]. Although these schemes were designed for the Gaussian channel they show reasonable diversity when the number of states exceeds 16.

All the above TCM schemes have a spectral efficiency of two bits per symbol. The spectral efficiency can be increased by using Ungerboeck's [4] multidimensional QAM trellis codes, but their inherent diversity is very bad due to uncoded bits, which induce parallel transitions in the trellis [1].

Signal constellations having lattice structure are commonly accepted as good means for transmission with high spectral efficiency. The problem of finding good signal constellations for the Gaussian channel can be restated in terms of lattice sphere packings. Good lattice constellations for the Gaussian channel can be carved from lattices with high sphere packing density [6]. The linear and highly symmetrical structure of lattices usually simplifies the decoding task.

For the Rayleigh fading channel the basic ideas remain the same. The problem is to construct signal constellations with minimum average energy for a desired error rate, given the spectral efficiency. A very interesting approach has been recently proposed [8], [9], which makes use of some results of algebraic number theory. Using totally real algebraic number fields, some good lattice constellations matched to the Rayleigh fading channel, up to dimension eight, are found. The effectiveness of these constellations lies in their high degree of diversity, which is actually the maximum possible. By diversity we mean the number of different values in the components of any two distinct points of the constellation.

The signal constellations for the Gaussian channel are usually very bad when used over the Rayleigh fading channel since they have small diversity. On the other hand, the signal constellations in [9] matched to the Rayleigh fading channel are usually very bad when used over the Gaussian channel since the sphere packing density of these lattices is low. In this paper we search for lattice constellations which have good performance on both Gaussian and Rayleigh fading channel. The same constellations may be used for the Ricean channel which stands between the Gaussian and the Rayleigh channels.

The practical interest in such signal constellations rises from the need to transmit information over both terrestrial and satellite links. The same modulation/demodulation device can be used to communicate over the terrestrial link (between a mobile and a base station) and over the satellite link (between a mobile and a satellite). Lattice constellations matched to fading channels can also be applied in wireless local area networks (over the indoor channel) and asynchronous digital subscriber lines (over the phone line) [24]–[26]. The cable channel, combined with a multicarrier modulator and an interleaver, acts as a flat fading channel.

The paper outline is as follows. In Section II we show the system model and give the basic definitions. In Section III we analyze the error probability bounds to find an effective approach to the search for good constellations. The final target of this work is to find good constellations for the Gaussian and the Rayleigh fading channels; we will present two different approaches. The first (Sections VI and V), considers some constellations constructed for the fading channel and trades some of their diversity for a higher asymptotic gain

Manuscript received November 16, 1994; revised September 11, 1995. The material in this paper was presented in part at the International Symposium on Information Theory, Whistler, BC, Canada.

J. Boutros and J.-C. Belfiore are with the Ecole Nationale Supérieure des Télécommunications, Paris XIII, France.

C. Rastello (deceased) was with the Ecole Nationale Supérieure des Télécommunications, Paris XIII, France.

E. Viterbo is with the Politecnico di Torino, Torino, Italy.

Publisher Item Identifier S 0018-9448(96)01018-8.

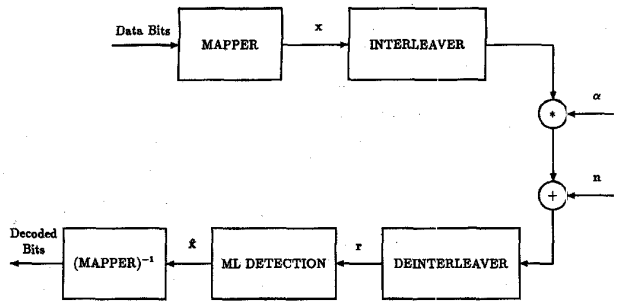

Fig. 1. The transmission system.

over the Gaussian channel. These constellations are obtained using some results in algebraic number theory, which will be presented in the various subsections. The second approach (Section VI) goes in the opposite direction: starting from good constellations for the Gaussian channel we try modifying them to increase their diversity. In this section we will need some further results in algebraic number theory related to ideals and their factorization. Section VII will illustrate the decoding algorithm used with these lattice constellations together with practical results. Finally, in Section VIII we discuss the two different approaches to establish which one is the most effective.

II. System Model and Terminology

The baseband transmission system is shown in Fig. 1. The mapper associates an m-uple of input bits to a signal point $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ in the n-dimensional Euclidean space $\boldsymbol{R}^n$. Let $M = 2^m$ be the total number of signal points in the constellation. An interleaver precedes the channel in the system model. It interleaves the real components of the sequence of mapped points. The constellation points are transmitted either over an additive white Gaussian noise (AWGN) channel, giving $\boldsymbol{r} = \boldsymbol{x} + \boldsymbol{n}$ or over an independent Rayleigh fading channel (RFC) giving $\boldsymbol{r} = \boldsymbol{\alpha} * \boldsymbol{x} + \boldsymbol{n}$, where $\boldsymbol{r}$ is the received point, $\boldsymbol{n} = (n_1, n_2, \cdots, n_n)$ is a noise vector, whose real components n_i are zero-mean, N_0 variance Gaussian distributed independent random variables, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots \alpha_n)$ are the random fading coefficients with unit second moment, and $*$ represents the componentwise 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. The independence of the fading samples represents the situation where the components of the transmitted points are perfectly interleaved. We note that in the case of totally complex lattices (Sections IV-C and VI), interleaving can be done symbol by symbol instead of componentwise.

The M transmitted signals $\boldsymbol{x}$ are chosen from a finite constellation S which is carved from a lattice Λ. In particular, the points of the constellation are chosen among the first shells of the lattice, so that the signal set approaches the optimal spherical shape. Each point is labeled with an m-bit binary label. The spectral efficiency will be measured in number of bits per two dimensions

$$\eta = \frac{2m}{n}$$

and the signal-to-noise ratio per bit is given by

$$\text{SNR} = \frac{E_b}{N_0}$$

where E_b is the narrowband average energy per bit and $N_0/2$ is the narrowband noise power spectral density. Let $E = E[\|\boldsymbol{x}\|^2]$ be the average baseband energy per point of the constellation. The equality $E_b = 0.5 * E/m = E/(n * \eta)$ is very useful to relate the SNR to the constellation's second moment.

After de-interleaving the components of the received points, the maximum-likelihood detection criterion imposes the minimization of the following metric:

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

for AWGN channel and

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

for Rayleigh fading channel with perfect side information. Using this criterion we obtain the decoded point $\hat{\boldsymbol{x}}$ from which the decoded bits are extracted.

III. Searching for Optimal Lattice Constellations

To address the search for good constellations we need an estimate of the error probability of the above system.

Since a lattice is *geometrically uniform* we may simply write $P_e(\Lambda) = P_e(\Lambda|\boldsymbol{x})$ for any transmitted point $\boldsymbol{x} \in \Lambda$. For convenience, $\boldsymbol{x}$ is usually taken to be the all zero vector $\boldsymbol{0}$. We now apply the union bound which gives an upper bound to the point error probability

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{\boldsymbol{y} \neq \boldsymbol{x}} P(\boldsymbol{x} \to \boldsymbol{y}) \tag{3}$$

where $P(\boldsymbol{x} \to \boldsymbol{y})$ is the pairwise error probability, the probability that the received point is "closer" to $\boldsymbol{y}$ than to $\boldsymbol{x}$ according to the metric defined in (1) or (2), when $\boldsymbol{x}$ is transmitted. The first inequality takes into account the edge effects of the finite constellation S compared to the infinite lattice Λ.

For the AWGN channel, (3) simply becomes [6, ch. 3]

$$P_e(\Lambda) \leq \frac{\tau}{2} \operatorname{erfc}\left(\frac{d_{E\min}/2}{\sqrt{2N_0}}\right) \tag{4}$$

where τ is the *kissing number* and $d_{E\min}$ is the *minimum Euclidean distance* of the lattice. The error probability per point of a cubic constellation can be easily upper-bounded (see Appendix I) with a function of the signal-to-noise ratio given by

$$P_e(S) \leq \frac{\tau}{2} \operatorname{erfc}\left(\sqrt{\frac{3\eta}{2^{\eta+1}} \frac{E_b}{N_0} \gamma(\Lambda)}\right) \tag{5}$$

where

$$\gamma(\Lambda) = \frac{d^2_{E\min}}{\mathrm{vol}\,(\Lambda)^{2/n}} \tag{6}$$

is the *fundamental gain* of Λ. We recall that $\gamma(\boldsymbol{Z}^n) = 1(\boldsymbol{Z}^n$ is the n-dimensional integer grid lattice), so that $\gamma(\Lambda)$ is the asymptotic gain of Λ over $\boldsymbol{Z}^n$. For spherical constellations the total gain should also take into account the shape gain.

For the Rayleigh fading channel, the standard Chernoff bound technique [1] or the direct computation using the Gaussian tail function approximation (see Appendix II), give an estimate of the pairwise error probability

$$P(\boldsymbol{x} \to \boldsymbol{y}) \le \frac{1}{2} \prod_{i=1}^{n} \frac{1}{1 + \dfrac{(x_i - y_i)^2}{8N_0}} \tag{7}$$

and for large signal-to-noise ratios

$$\begin{aligned} P(\boldsymbol{x} \to \boldsymbol{y}) &\le \frac{1}{2} \prod_{x_i \neq y_i} \frac{1}{\dfrac{(x_i - y_i)^2}{8N_0}} \\ &= \frac{1}{2} \frac{1}{\left(\dfrac{\eta}{8}\dfrac{E_b}{N_0}\right)^{l} d_p^{(l)}(\boldsymbol{x}, \boldsymbol{y})^2} \end{aligned} \tag{8}$$

where $d_p^{(l)}(\boldsymbol{x}, \boldsymbol{y})$ is the (normalized) *l-product distance* of $\boldsymbol{x}$ from $\boldsymbol{y}$ when these two points differ in l components

$$d_p^{(l)}(\boldsymbol{x}, \boldsymbol{y})^2 = \frac{\prod\limits_{x_i \neq y_i} (x_i - y_i)^2}{(E/n)^l}. \tag{9}$$

Asymptotically, (3) is dominated by the term $1/(E_b/N_0)^L$ where L is the minimum number of different components of any two distinct constellation points. L is the so-called *diversity* of the signal constellation.

In general, rearranging (3) we obtain

$$P_e(\Lambda) \le \frac{1}{2} \sum_{l=L}^{n} \frac{K_l}{\left(\dfrac{\eta}{8}\dfrac{E_b}{N_0}\right)^{l}} \tag{10}$$

where

$$K_l = \sum_{d_p^{(l)}} A_{d_p^{(l)}} / (d_p^{(l)})^2 .\ A_{d_p^{(l)}}$$

is the number of points $\boldsymbol{y}$ at l-product distance $d_p^{(l)}$ from $\boldsymbol{x}$ and with l different components, $L \le l \le n$. The series in K_l can be interpreted as a *theta series* of the lattice [6], when the product distance is considered instead of the Euclidean distance.

In (10) we find all the ingredients to obtain a low error probability at a given signal-to-noise ratio E_b/N_0. In order of relevance we have to

1) maximize the diversity $L = \min(l)$;
2) minimize the average energy per constellation point E;
3) minimize K_l and especially take care of

$$d_{p,\min} = \min(d_p^{(L)}(\boldsymbol{x}, \boldsymbol{y}))$$

and $\tau_p = A_{d_p^{(L)}}$, the kissing number for the L-product distance.

The terms in (10) clearly become less important when l increases, but the values of $A_{d_p^{(l)}}$ and $d_p^{(l)}(\boldsymbol{x}, \boldsymbol{y})$ should be taken into account for nonasymptotic considerations.

In fact, the asymptotic coding gain of a system-2 over a reference system-1, having the same spectral efficiency and the same diversity L is given by

$$\gamma_{\text{asympt.}} = \left(\frac{K_L(1)}{K_L(2)}\right)^{1/L} \tag{11}$$

with the definitions given above. In general, the asymptotic coding gain may not be defined for systems with different diversities L_1 and L_2; in such cases the coding gain varies with the signal-to-noise ratio.

In the sequel of this paper, we limit our search for optimal constellations, with high diversity and low energy, to the class of lattices constructed from algebraic number fields.

IV. Lattices from Algebraic Number Fields

In the following, we will assume that the reader is familiar with the basic definitions on lattices (see [6]) and we show the way to construct lattices from algebraic number fields. We will present only the strictly relevant definitions and results in algebraic number theory, which lead to the lattice construction. The exposition is self-contained and is based on simple examples, but the interested reader may consult any book on algebraic number theory to quench their thirst for rigor (e.g., [13]–[15]). The basic ideas and definitions of Section IV are as follows:

- The number field K and its ring of integers O_K.
- The primitive element θ such that $K = \boldsymbol{Q}(\theta)$ and its minimal polynomial $\mu_\theta(x)$.
- The integral basis $(\omega_1, \omega_2, \cdots, \omega_n)$ of K giving $O_K = \boldsymbol{Z}[\omega_1, \omega_2, \cdots, \omega_n]$.
- The n $\boldsymbol{Q}$-isomorphisms σ_i defined by $\sigma_i(\theta) = \theta_i$ the ith root of $\mu_\theta(x)$ and the canonical embedding σ: $K \to \boldsymbol{R}^n$.
- The two special cases of totally real lattices (θ_i's totally real) and totally complex lattices (θ_i's totally complex).

A. Algebraic Number Fields

Let $\boldsymbol{Z}$ be the ring of rational integers and let K be a field containing $\boldsymbol{Q}$, the field of rational numbers. Algebraic number theory studies the properties of such fields in relation to the solution of algebraic equations.

Definition 1: Let α be an element of K, we say that α is an **algebraic number** if it is a root of a monic polynomial with coefficients in $\boldsymbol{Q}$. Such polynomial with lowest degree is called the minimal polynomial of α and denoted $\mu_\alpha(x)$. If all the elements of K are algebraic we say that K is an **algebraic extension** of $\boldsymbol{Q}$.

Example 1: Let us consider the field $K = \{a + b\sqrt{2}$ with $a, b \in \boldsymbol{Q}\}$. It is simple to see that K is a field containing $\boldsymbol{Q}$ and that any $\alpha \in K$ is a root of the polynomial $\mu_\alpha(x) = x^2 - 2ax + a^2 - 2b^2$ with rational coefficients. We conclude that K is an algebraic extension of $\boldsymbol{Q}$.

Definition 2: We say that $\alpha \in K$ is an **algebraic integer** if it is a root of a monic polynomial with coefficients in $\boldsymbol{Z}$. The set of algebraic integers of K is a ring called the **ring of integers** of K and is indicated with O_K.

Example 1 (Continued): In our example, all the algebraic integers will take the form $a+b\sqrt{2}$ with $a, b \in \boldsymbol{Z}$. Care should be taken in generalizing this result (see Example 3). O_K is a ring contained in K since it is closed under all operations except for the inversion. For example, $(2+2\sqrt{2})^{-1} = (2-\sqrt{2})/6$ does not belong to O_K.

Definition 3: We define the **degree** $[K:\boldsymbol{Q}]$ of an algebraic extension K of $\boldsymbol{Q}$ as the dimension of K when considered as a vector space over $\boldsymbol{Q}$. An **algebraic number field** is an algebraic extension of $\boldsymbol{Q}$ of finite degree.

Example 1 (Continued): K is a vector space over $\boldsymbol{Q}$ of dimension 2 so it is an algebraic number field of degree 2 (a quadratic field). This is one way of seeing algebraic number fields: as finite dimensional vector spaces over $\boldsymbol{Q}$.

Result 1: Let K be an algebraic number field. There exists an element $\theta \in K$, called **primitive element**, such that the $\boldsymbol{Q}$ vector space K is generated by the powers of θ. If K has degree n then $(1, \theta, \theta^2, \cdots, \theta^{n-1})$ is a **basis** of K and $\deg(\mu_\theta(x)) = n$. We will write $K = \boldsymbol{Q}(\theta)$.

Example 1 (Continued): In the above example we have $K = \boldsymbol{Q}(\sqrt{2})$. $\theta = \sqrt{2}$ is a primitive element since $(1, \sqrt{2})$ form a basis. The minimal polynomial is $\mu_\theta(x) = x^2 - 2$.

Example 2: Let us consider a slightly more complex example with K generated by $\sqrt{2}$ and $\sqrt{3}$; all its elements may be written as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \boldsymbol{Q}$ so that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a basis of K. If we consider the element $\theta = \sqrt{2} + \sqrt{3}$, we have

$$(1, \theta, \theta^2, \theta^3) = (1, \sqrt{2}, \sqrt{3}, \sqrt{6}) \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

The transition matrix is invertible in $\boldsymbol{Q}$ proving that we can write $K = \boldsymbol{Q}(\theta)$. The minimal polynomial of θ is $x^4 - 10x^2 + 1$ and its roots are

$$\theta = \sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}.$$

In this particular case they are all primitive elements.

The problem of finding the primitive element given a basis is in general very complex. Usually we start from a field defined by its primitive element.

Result 2: There exists a primitive element θ which is an algebraic integer of K. In other words, the minimal polynomial $\mu_\theta(x)$ has coefficients in $\boldsymbol{Z}$.

In the above examples θ is not only a primitive element but also an algebraic integer.

B. Integral Basis and Canonical Embedding

In the special case $K = \boldsymbol{Q}(\sqrt{2})$, we have seen that the ring of integers O_K was the set of all elements $a + b\sqrt{2}$ with a, b integers. $O_K = \boldsymbol{Z}(\sqrt{2})$ is a vector space over $\boldsymbol{Z}$ with $(1, \sqrt{2})$ as a basis. O_K is called a *$\boldsymbol{Z}$-module*, since $\boldsymbol{Z}$ is a ring and not a field.

Result 3: The ring of integers O_K of K forms a $\boldsymbol{Z}$-module of rank n (a linear vector space of dimension n over $\boldsymbol{Z}$).

Definition 4: Let $(\omega_1, \omega_2, \cdots, \omega_n)$ be a basis of K. We say that (ω_i) is an **integral basis** of K if $O_K = \boldsymbol{Z}(\omega_1, \omega_2, \cdots, \omega_n)$, that is, if (ω_i) is a generating set of the $\boldsymbol{Z}$-module O_K. So that we can write any element of O_K as $\Sigma_{i=1}^n a_i\omega_i$ with $a_i \in \boldsymbol{Z}$.

Example 3: Take $K = \boldsymbol{Q}(\sqrt{5})$; we know that any algebraic integer β in K has the form $a + b\sqrt{5}$ with $a, b \in \boldsymbol{Q}$ such that the polynomial $\mu_\beta(x) = x^2 - 2ax + a^2 - 5b^2$ has integer coefficients. By simple arguments it can be shown that all the elements of O_K take the form $\beta = (u + v\sqrt{5})/2$ with both u, v integers with the same parity. So we can write $\beta = h + k(1 + \sqrt{5})/2$ with $h, k \in \boldsymbol{Z}$. This shows that $(1, (1 + \sqrt{5})/2)$ is an integral basis. The basis $(1, \sqrt{5})$ is not integral since $a + b\sqrt{5}$ with $a, b \in \boldsymbol{Z}$ is only a subset of O_K. Incidently, $(1 + \sqrt{5})/2$ is also a primitive element of K with minimal polynomial $x^2 - x - 1$.

There exist efficient algorithms to find an integral basis of a given algebraic number field in polynomial time [11], [12].

Definition 5: Let K and K' be two fields containing $\boldsymbol{Q}$, we call $\phi : K \to K'$ a **$\boldsymbol{Q}$-homomorphism** if for each $a \in \boldsymbol{Q}, \phi(a) = a$. If $K' = \boldsymbol{C}$, the field of complex numbers, a $\boldsymbol{Q}$-homomorphism $\phi : K \to \boldsymbol{C}$ is called an **embedding** of K into $\boldsymbol{C}$.

Result 4: Let θ be a primitive element of K and $\mu_\theta(x)$ its minimal polynomial with roots $(\theta_1, \theta_2, \cdots, \theta_n), \theta = \theta_1$. There are exactly n embeddings of K into $\boldsymbol{C}$. Each embedding $\sigma_i : K \to \boldsymbol{C}, \sigma_i(\theta) = \theta_i$, is completely identified by a root $\theta_i \in \boldsymbol{C}$ of $\mu_\theta(x)$.

Notice that $\sigma_1(\theta) = \theta_1 = \theta$ and thus σ_1 is the identity mapping $\sigma_1(K) = K$. When we apply the embedding σ_i to an arbitrary element α of K using the properties of $\boldsymbol{Q}$-homomorphisms we have

$$\sigma_i(\alpha) = \sigma_i\left(\sum_{k=1}^n a_k\theta^k\right) = \sum_{k=1}^n \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^n a_k\theta_i^k \in \boldsymbol{C}$$

and we see that the image of any α under σ_i is uniquely identified by θ_i.

Definition 6: The elements $\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)$ are called the **conjugates** of α and

$$N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$$

is the **algebraic norm** of α.

Result 5: For any $\alpha \in K$, we have $N(\alpha) \in \boldsymbol{Q}$. If $\alpha \in O_K$ we have $N(\alpha) \in \boldsymbol{Z}$.

Example 1 (Continued): The roots of the minimal polynomial $x^2 - 2$ are $\theta_1 = \sqrt{2}$ and $\theta_2 = -\sqrt{2}$ then

$$\sigma_1(\theta) = \sqrt{2} \quad \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$$
$$\sigma_2(\theta) = -\sqrt{2} \quad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.$$

The algebraic norm of α is $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 - 2b^2$ and we can verify the above result.

Definition 7: Let $(\omega_1, \omega_2, \cdots, \omega_n)$ be an integral basis of K. The **absolute discriminant** of K is defined as $d_K = \det[\sigma_j(\omega_i)]^2$.

Result 6: The absolute discriminant belongs to $\boldsymbol{Z}$.

Example 3 (Continued): Applying the two $\boldsymbol{Q}$-homomorphisms to the integral basis ω_1, ω_2, we obtain

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

Definition 8: Let $(\sigma_1, \sigma_2, \cdots \sigma_n)$ be the n $\boldsymbol{Q}$-homomorphisms of K into $\boldsymbol{C}$. Let r_1 be the number of $\boldsymbol{Q}$-homomorphisms with image in $\boldsymbol{R}$, the field of real numbers, and $2r_2$ the number of $\boldsymbol{Q}$-homomorphisms with image in $\boldsymbol{C}$ so that

$$r_1 + 2r_2 = n.$$

The pair (r_1, r_2) is called the **signature** of K. If $r_2 = 0$ we have a **totally real** algebraic number field. If $r_1 = 0$ we have a **totally complex** algebraic number field. In all other cases we will speak about a complex algebraic number field.

Example 4: All the previous examples were totally real algebraic number fields with $r_1 = n$. Let us now consider $K = \boldsymbol{Q}(\sqrt{-3})$. The minimal polynomial of $\sqrt{-3}$ is $x^2 + 3$ and has two complex roots so the signature of K is $(0, 1)$. For later use we observe that $(1, \sqrt{-3})$ is not an integral basis. If we take

$$\theta = e^{i\pi/3} = (1 + i\sqrt{3})/2$$

where $i = \sqrt{-1}$, we have

$$K = \boldsymbol{Q}(\theta) = \boldsymbol{Q}(\sqrt{-3})$$

and an integral basis is $(1, (1 + i\sqrt{3})/2)$. The minimal polynomial of θ is $x^2 - x + 1$. The ring of integers of this field is also known as the Eisenstein integer ring. This is the simplest example of *cyclotomic field*, i.e., a field generated by an mth root of unity.

Definition 9: Let us order the σ_i so that $\sigma_i(\alpha) \in \boldsymbol{R}$ for $1 \le i \le r_1$ and $\sigma_{j+r_2}(\alpha)$ is the complex conjugate of $\sigma_j(\alpha)$ for $r_1 + 1 \le j \le r_1 + r_2$. We call **canonical embedding** $\sigma : K \to \boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$ the isomorphism defined by

$$\sigma(\alpha) = (\sigma_1(\alpha) \cdots \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \cdots, \sigma_{r_1+r_2}(\alpha)) \in \boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}.$$

If we identify $\boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$ with $\boldsymbol{R}^n$, the canonical embedding can be rewritten as $\sigma: K \to \boldsymbol{R}^n$

$$\sigma(\alpha) = (\sigma_1(\alpha), \cdots, \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \cdots, \Re\sigma_{r_1+r_2}(\alpha), \Im\sigma_{r_1+r_2}(\alpha)) \in \boldsymbol{R}^n$$

where $\Re$ is the real part and $\Im$ is the imaginary part.

This definition establishes a one-to-one correspondence between the elements of an algebraic number field of degree n and the vectors of the n-dimensional Euclidean space. The final step for this algebraic construction of a lattice is given by the following result.

Result 7: Let $(\omega_1, \omega_2, \cdots, \omega_n)$ be an integral basis of K and let d_K be the absolute discriminant of K. The n vectors $\boldsymbol{v}_i = \sigma(\omega_i) \in \boldsymbol{R}^n$ are linearly independent, so they define a full rank lattice $\Lambda = \sigma(O_K)$ with generator matrix (see (12) at the bottom of this page).

The vectors $\boldsymbol{v}_i$ are the rows of G. The volume of the fundamental parallelotope of Λ is given by [13]

$$\text{vol}\,(\Lambda) = |\det(G)| = 2^{-r_2} \times \sqrt{|d_K|}. \tag{13}$$

C. Totally Real and Totally Complex Number Fields

Result 8: The lattices obtained from the generator matrix (12) exhibit a diversity $L = r_1 + r_2$.

Proof: Let $\boldsymbol{z} \neq \boldsymbol{o}$ be an arbitrary point of Λ

$$\boldsymbol{z} = (z_1, z_2, \cdots, z_n) = \sum_{i=1}^{n} \lambda_i \boldsymbol{v}_i$$

with $\lambda_i \in \boldsymbol{Z}$ and $\boldsymbol{v}_i = (v_{ij}) = \sigma(\omega_i)$ the rows of the lattice generator matrix G.

$$\begin{aligned} \prod_{j=1}^{n} |z_j| &= \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| \\ &= \prod_{j=1}^{r_1} \left| \sigma_j\left(\sum_{i=1}^{n} \lambda_i \omega_i\right) \right| \times \prod_{j=r1+1}^{r_1+r_2} \left| \Re\sigma_j\left(\sum_{i=1}^{n} \lambda_i \omega_i\right) \right| \\ &\quad \times \prod_{j=r1+1}^{r_1+r_2} \left| \Im\sigma_j\left(\sum_{i=1}^{n} \lambda_i \omega_i\right) \right| \end{aligned} \tag{14}$$

The algebraic integer $\Sigma_{i=1}^{n} \lambda_i \omega_i$ is nonzero because all λ_i's are not null together ($z \neq 0$). This implies that $\sigma_j(\Sigma_{i=1}^{n} \lambda_i \omega_i) \neq 0$ and so the first product at the right side of the above expression contains exactly r_1 nonzero factors. The minimum number of nonzero factors in the second and the third products is r_2 since the real and imaginary parts of any one of the complex embeddings may not be null together. We then conclude that for such lattices we have a diversity $L \ge r_1 + r_2$. Now, let us take the special element $\alpha = 1$ in O_K. The canonical embedding applied to 1 gives exactly $r_1 + r_2$ nonzero terms in the above product ($\sigma_j(1) = 1$ for any j). Hence, we can

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \cdots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \cdots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \cdots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\omega_n) & \cdots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \cdots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix} \tag{12}$$

confirm that $L = r_1 + r_2$, as indicated in [10]. Q.E.D.

$$\frac{d_{E\min}/2}{\sqrt{2N_0}} = \sqrt{\frac{d^2_{E\min}}{8N_0}} = \sqrt{\frac{3\eta}{2^{\eta+1}}\frac{E_b}{N_0}\frac{d^2_{E\min}}{\mathrm{vol}\,(\Lambda)^{2/n}}}.$$

In the case of totally real algebraic number fields ($r_2 = 0$), presented in [9], we have

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \cdots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \cdots & \sigma_n(\omega_n) \end{pmatrix}.$$

The lattice Λ constructed in this case attains the maximum degree of diversity $L = n$. The n-product distance of $\boldsymbol{z}$ from $\mathbf{0}$ is

$$d_p^n(\mathbf{0}, \boldsymbol{z}) = \prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left|\sum_{i=1}^{n} \lambda_i v_{ij}\right| = \prod_{j=1}^{n} \left|\sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i)\right| = \prod_{j=1}^{n} \left|\sigma_j\left(\sum_{i=1}^{n} \lambda_i \omega_i\right)\right| = \left|N\left(\sum_{i=1}^{n} \lambda_i \omega_i\right)\right|. \quad (15)$$

Since $\Sigma_{i=1}^{n} \lambda_i \omega_i \in O_K$ and it is different from zero, according to Result 5, we have

$$d_p^{(n)}(\mathbf{0}, \boldsymbol{z}) \geq 1 \quad \forall \boldsymbol{z} \neq \mathbf{0}.$$

The minimum product distance $d_{p,\min} = 1$ is given by the elements of K with algebraic norm 1, the so-called *units* of K. The fundamental parallelotope has volume

$$\mathrm{vol}\,(\Lambda) = \sqrt{|d_K|}.$$

The totally real algebraic number fields with minimum absolute discriminant are known up to dimension 8 (first column of Table I) and appear to be the best asymptotically good lattices for the Rayleigh fading channel. In fact, for a fixed number of points M, the energy of constellations carved from these lattices is proportional to $\mathrm{vol}\,(\Lambda)$ and $\mathrm{vol}\,(\Lambda)$ is minimized by selecting the fields with minimum absolute discriminants.

Still, two disadvantages are hidden behind the maximal diversity and the minimal absolute discriminant. The fundamental volume can be further reduced if we choose a signature where $r_2 \neq 0$, i.e. if the number field is complex. Equation (14) shows that $\mathrm{vol}\,(\Lambda)$ can be divided by 2^{r_2}. We can even maximize r_2 by working in a totally complex field $r_2 = n/2$. Lattices derived from totally real number fields have bad performance over a Gaussian channel (a negative fundamental gain as shown in Section VII) mainly because of their high values of $\mathrm{vol}\,(\Lambda)$ (Table I). The second disadvantage appears over the fading channel and is related to the product kissing number τ_p. We find that the product kissing number is much higher for real fields lattices than for complex fields lattices.

High diversity dense lattices built from complex algebraic number fields have been first proposed in [10]. The totally complex fields are possible only for even degrees since $r_2 = n/2$. The generator matrix is

$$G = \begin{pmatrix} \Re\sigma_1(\omega_1) & \Im\sigma_1(\omega_1) & \cdots & \Re\sigma_{r_2}(\omega_1) & \Im\sigma_{r_2}(\omega_1) \\ \Re\sigma_1(\omega_2) & \Im\sigma_1(\omega_2) & \cdots & \Re\sigma_{r_2}(\omega_2) & \Im\sigma_{r_2}(\omega_2) \\ \vdots & & & & \vdots \\ \Re\sigma_1(\omega_n) & \Im\sigma_1(\omega_n) & \cdots & \Re\sigma_{r_2}(\omega_n) & \Im\sigma_{r_2}(\omega_n) \end{pmatrix}. \quad (16)$$

Nothing can be said about the value of the minimum product distance $d_{p,\min}$ for complex fields lattices, since it is not related to the algebraic norm as in the totally real case.

Looking at Table I we immediately notice that the absolute discriminants of the complex fields are comparatively smaller than the ones for the totally real fields. This fact, combined with the fact that $\mathrm{vol}\,(\Lambda)$ is reduced by a factor 2^{-r_2}, results in lower average energy of the constellation S, for complex fields. Of course, the price to pay is the reduced diversity unless we use number fields with higher degrees such as 12, 16 or 24. This led us to search for good lattices (Λ_{16} or Λ_{24}) adapted to Rayleigh channel and the logical continuation is Section VI. In the next section, we study in detail some of the lattices constructed by canonical embedding applied to fields in Tables I and II.

TABLE I
MINIMAL ABSOLUTE DISCRIMINANTS
(Values with an * are the best known values.)

n	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$	$r_2 = 3$	$r_2 = 4$
2	5	−3	—	—	—
3	49	−23	—	—	—
4	725	−275	117	—	—
5	14641	−4511	1609	—	—
6	300125	−92779*	28037*	−9747	—
7	20134393	?	?	?	—
8	282300416	?	?	?	1257728*

V. LATTICES FROM MINIMAL ABSOLUTE DISCRIMINANT FIELDS

In Table I we have all the known minimal absolute discriminant fields up to dimension 8. These fields (especially in dimensions above 4) have been a subject of study of a branch of mathematics known as *computational algebraic number theory*. Computational algebraic number theory has developed powerful algorithmic tools which enable to extend many results, with the aid of computers, to fields of higher degree [11], [12]. Part of this table, up to $n = 6$, can be found in [15] and the references therein. All the totally real fields are reported in [9]. For degree 5 and 6 complex fields see [16] and [17], respectively. The degree 8, totally complex field of minimal absolute discriminant can be found in [18] together with other 25 totally complex fields of absolute discriminant smaller than 1954287. Table II gives the *reduced* minimal polynomials of the fields of Table I along with the fundamental volume of the corresponding lattice obtained from the canonical embedding. A minimal polynomial is called *reduced* if the powers of one of its roots (the primitive element)

TABLE II
REDUCED MINIMAL POLYNOMIALS AND FUNDAMENTAL VOLUMES OF THE CORRESPONDING LATTICES

	$\mu_\theta(x)$	$vol(\Lambda_{n,L})$
$\Lambda_{2,1}$	x^2-x+1	0.8660
$\Lambda_{2,2}$	x^2-x-1	2.2361
$\Lambda_{3,2}$	x^3-x-1	2.3979
$\Lambda_{3,3}$	x^3+x^2-2x-1	7
$\Lambda_{4,2}$	$x^4-x^3-x^2+x+1$	2.7042
$\Lambda_{4,3}$	x^4-x^3+2x-1	8.2916
$\Lambda_{4,4}$	$x^4-x^3-3x^2+x+1$	26.9258
$\Lambda_{5,3}$	$x^5-x^3+x^2+x-1$	10.0281
$\Lambda_{5,4}$	$x^5-2x^3+x^2-1$	33.5820
$\Lambda_{5,5}$	$x^5+x^4-4x^3-3x^2+3x+1$	121
$\Lambda_{6,3}$	$x^6-3x^5+4x^4-4x^3+4x^2-2x+1$	12.3409
$\Lambda_{6,4}$	$x^6-2x^5+3x^3-2x-1$	41.8606
$\Lambda_{6,5}$	$x^6+x^5-2x^4-3x^3-x^2+2x+1$	152.2982
$\Lambda_{6,6}$	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	547.8367
$\Lambda_{7,7}$	$x^7+x^6-6x^5-5x^4+8x^3+5x^2-2x-1$	4487.1364
$\Lambda_{8,4}$	$x^8-2x^7+4x^5-4x4+3x^2-2x+1$	70.0928
$\Lambda_{8,8}$	$x^8+2x^7-7x^6-8x^5+15x^4+8x^3-9x^2-2x+1$	16801.7980

is an integral basis of the number field. These lattices will be indicated with $\Lambda_{n,L}$.

The main steps for the construction of a lattice from an algebraic number field $K=\boldsymbol{Q}(\theta)$ can be summarized as follows:

- Find an integral basis of K, which identifies O_K.
- Find the n roots of $\mu_\theta(x)$, which identify the n embeddigs $\sigma_1,\sigma_2,\cdots,\sigma_n$.
- Construct the generator matrix applying the canonical embedding.

We show the application of this procedure to some of the lattices of Table II.

$\Lambda_{2,1}-K=\boldsymbol{Q}(i\sqrt{3})$

From Example 4 we have the integral basis $(1,1+i\sqrt{3}/2)$. The two embeddings are

$$\sigma_1(i\sqrt{3})=i\sqrt{3},\sigma_2(i\sqrt{3})=-i\sqrt{3}$$

and the lattice generator matrix is

$$G=\begin{pmatrix}\Re\sigma_1(1) & \Im\sigma_1(1)\\ \Re\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right) & \Im\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right)\end{pmatrix}=\begin{pmatrix}1 & 0\\ \frac{1}{2} & \frac{\sqrt{3}}{2}\end{pmatrix}.$$

We may recognize in the above matrix the *hexagonal lattice* A_2. The fundamental volume is $\mathrm{vol}\,(\Lambda_{2,1})=|\det(G)|=\sqrt{3}/2$ and the minimum squared Euclidean distance is $d^2_{E\,\min}=1$. $r_1=0,r_2=1$ and the diversity is $L=1$ since the vector $(1,0)$ belongs to the lattice.

$\Lambda_{2,2}-K=\boldsymbol{Q}(\sqrt{5})$

From Example 3 we have the integral basis $(1,1+\sqrt{5}/2)$. The two embeddings are $\sigma_1(\sqrt{5})=\sqrt{5},\sigma_2(\sqrt{5})=-\sqrt{5}$ and the lattice generator matrix is

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

The fundamental volume is $\mathrm{vol}\,(\Lambda_{2,2})=|\det(G)|=\sqrt{5}$ and the minimum squared Euclidean distance is $d^2_{E\,\min}=2$. $r_1=2,r_2=0$ and the diversity is $L=2$.

$\Lambda_{3,2}-K=\boldsymbol{Q}(\theta)$

θ is a primitive element with minimal polynomial x^3-x-1, whose roots are

$$\theta_1=U+V\ \theta_{2,3}=-\frac{1}{2}(U+V)\pm i\frac{\sqrt{3}}{2}(U-V)$$

where

$$U=\frac{1}{3}\sqrt[3]{\frac{9+3\sqrt{63}}{2}}\quad V=\frac{1}{3}\sqrt[3]{\frac{9-3\sqrt{63}}{2}}.$$

The primitive element θ coincides with θ_2 and an integral basis is $1,\theta,\theta^2$. The three embeddings are $\sigma_1(\theta)=\theta_1$ (real), $\sigma_2(\theta)=\theta_2$, and $\sigma_3(\theta)=\theta_3$, where σ_2 and σ_3 are conjugates $(r_1=1,r_2=1)$. We obtain the lattice generator matrix (see the bottom of this page).

The fundamental volume is $\mathrm{vol}\,(\Lambda_{3,2})=|\det(G)|=2.39$ and the minimum squared Euclidean distance is $d^2_{E\,\min}=1.895$. The diversity is given by $L=r_1+r_2=2$ since the vector $(1,1,0)$ belongs to the lattice and $d^{(2)}_p((0,0,0),(1,1,0))=1$.

$\Lambda_{3,3}-K=\boldsymbol{Q}(cos\,(2\pi/7))$

An integral basis is

$$(2\cos(2\pi/7),2\cos(4\pi/7),2\cos(6\pi/7)).$$

$$G=\begin{pmatrix}1 & 1 & 0\\ (U+V) & -\frac{1}{2}(U+V) & \frac{\sqrt{3}}{2}(U+V)\\ (U+V)^2-4 & -\frac{1}{2}(U^2+V^2-4UV) & -\frac{\sqrt{3}}{2}(U^2-V^2)\end{pmatrix}=\begin{pmatrix}1.000 & 1.000 & 0.000\\ 1.325 & -0.662 & 0.562\\ 1.755 & 0.123 & -0.745\end{pmatrix}$$

With the following three embeddings:

$$\sigma_1(\cos(2\pi/7)) = \cos(2\pi/7)$$
$$\sigma_2(\cos(2\pi/7)) = \cos(4\pi/7)$$
$$\sigma_3(\cos(2\pi/7)) = \cos(6\pi/7)$$

we obtain the lattice generator matrix

$$G = \begin{pmatrix} 2\cos(2\pi/7) & 2\cos(4\pi/7) & 2\cos(6\pi/7) \\ 2\cos(4\pi/7) & 2\cos(6\pi/7) & 2\cos(2\pi/7) \\ 2\cos(6\pi/7) & 2\cos(2\pi/7) & 2\cos(4\pi/7) \end{pmatrix}$$

The fundamental volume is $\mathrm{vol}(\Lambda_{3,3}) = |\det(G)| = 7$ and the minimum squared Euclidean distance is $d^2_{E\,\min} = 3$. The diversity is $L = 3$.

$\Lambda_{4,2} - K = \boldsymbol{Q}(\theta)$

θ is a primitive element with minimal polynomial $x^4 + 2x^2 + 13$ and roots

$$\theta_{1,2,3,4} = \pm(R \pm iI) = \pm\left(\sqrt{\frac{\sqrt{13}-1}{2}} \pm i\sqrt{\frac{\sqrt{13}+1}{2}}\right).$$

Taking the following signs for the roots:

$$\theta_1 : (++),\ \theta_2 = (-+),\ \theta_3 : (+-),\ \theta_4 : (--)$$

we have the primitive element $\theta = \theta_1$ and the four embeddings

$$\sigma_1(\theta) = \theta_1,\ \sigma_2(\theta) = \theta_2,\ \sigma_3(\theta) = \theta_3,\ \sigma_4(\theta) = \theta_4.$$

The canonical embedding is given by

$$\sigma = (\Re\sigma_1,\ \Im\sigma_1,\ \Re\sigma_2,\ \Im\sigma_2)$$

but $(1, \theta, \theta^2, \theta^3)$ is not an integral basis, because x^4+2x^2+13 is not reduced. An integral basis is

$$(1, \tfrac{1}{2}(1+\theta), \tfrac{1}{4}(3+\theta^2), \tfrac{1}{8}(1+\theta)(3+\theta^2))$$

We obtain the lattice generator matrix:

$$G = \begin{pmatrix} 1.000 & 0.000 & 1.000 & 0.000 \\ 1.070 & -0.758 & -0.070 & -0.758 \\ 0.500 & -0.866 & 0.500 & 0.866 \\ -0.121 & -1.306 & 0.621 & -0.440 \end{pmatrix}$$

The fundamental volume is $\mathrm{vol}(\Lambda_{4,2}) = |\det(G)| = 2.70$ and the minimum squared Euclidean distance is $d^2_{E\,\min} = 2$. The diversity is given by $L = r_2 = 2$ since the vector $(1, 0, 1, 0)$ belongs to the lattice and $d_p^{(2)}((0,0,0,0),(1,0,1,0)) = 1$.

$\Lambda_{4,3} - K = \boldsymbol{Q}(i\sqrt{-3+2\sqrt{5}})$

The roots of the minimal polynomial $x^4 - 6x^2 - 11$ are

$$\theta_1 = \sqrt{3+2\sqrt{5}},$$
$$\theta_2 = -\sqrt{3+2\sqrt{5}},$$
$$\theta_3 = i\sqrt{-3+2\sqrt{5}}$$

and

$$\theta_4 = -i\sqrt{-3+2\sqrt{5}}.$$

With $\theta = \theta_3$, the four embeddings are $\sigma_1(\theta) = \theta_1, \sigma_2(\theta) = \theta_2, \sigma_3(\theta) = \theta_3$, and $\sigma_4(\theta) = \theta_4$ and the integral basis has the same form as in $\Lambda_{4,2}$. The canonical embedding is given by $\sigma = (\sigma_1, \sigma_2, \Re\sigma_3, \Im\sigma_3)$. We obtain the lattice generator matrix:

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 0.000 \\ 1.866 & -0.866 & 0.500 & -0.606 \\ 2.618 & 2.618 & 0.381 & 0.000 \\ 4.887 & -2.269 & 0.190 & -0.231 \end{pmatrix}.$$

As an example we show the calculation of the element $(4, 2)$ of the above matrix

$$\begin{aligned} \sigma_2(\tfrac{1}{8}(1+\theta)(3+\theta^2)) &= \sigma_2(\tfrac{1}{8})\sigma_2(1+\theta)\sigma_2(3+\theta^2) \\ &= \sigma_2(\tfrac{1}{8})(\sigma_2(1)+\sigma_2(\theta)) \\ &\quad \cdot(\sigma_2(3)+\sigma_2(\theta^2)) \\ &= \tfrac{1}{8}(1+\theta_2)(3+\theta_2^2) = -2.269 \end{aligned}$$

The fundamental volume is $\mathrm{vol}(\Lambda_{4,3}) = |\det(G)| = 8.29$ and the minimum squared Euclidean distance is $d^2_{E\,\min} = 2$. The diversity is given by $L = r_1 + r_2 = 3$ since the vector $(1, 1, 1, 0)$ belongs to the lattice and $d_p^{(3)}((0,0,0,0),(1,1,1,0)) = 1$.

$\Lambda_{4,4} - K = \boldsymbol{Q}(\sqrt{7+2\sqrt{5}})$

The roots of the minimal polynomial $x^4 - 14x^2 + 29$ are

$$\theta_1 = \sqrt{7+2\sqrt{5}}$$
$$\theta_2 = -\sqrt{7+2\sqrt{5}}$$
$$\theta_3 = \sqrt{7-2\sqrt{5}}$$

and

$$\theta_4 = -\sqrt{7-2\sqrt{5}}.$$

With $\theta = \theta_1$, the four embeddings are $\sigma_1(\theta) = \theta_1, \sigma_2(\theta) = \theta_2, \sigma_3(\theta) = \theta_3, \sigma_4(\theta) = \theta_4$, and an integral basis has the same form as in $\Lambda_{4,2}$. We obtain the lattice generator matrix

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 1.000 \\ -1.193 & -0.294 & 1.294 & 2.193 \\ 3.618 & 1.381 & 1.381 & 3.618 \\ -4.318 & -0.407 & 1.789 & 7.936 \end{pmatrix}.$$

The fundamental volume is $\mathrm{vol}(\Lambda_{4,4}) = |\det(G)| = 26.92$ and the minimum squared Euclidean distance is $d^2_{E\,\min} = 4$. According to Section IV-C, the diversity is 4 and $d_{p,min} = 1$.

VI. Lattices for the Gaussian Channel Adapted to the Fading Channel

The idea of rotating a QAM constellation in order to increase its diversity was first presented in [8]. The advantage of such a technique lays in the fact that the rotated constellation holds its properties over the Gaussian channel. The method proposed was straightforward: find the rotation angle which gives a diversity of 2 and maximizes the minimum product distance. It was found that for a 16-QAM the rotation angle of $\pi/8$ was optimum. Unfortunately, in dimensions greater than 2 this method becomes impracticable.

TABLE III
ASYMPTOTIC GAINS FOR THE GAUSSIAN CHANNEL

n	$r_2=0$	$r_2=1$	$r_2=2$	$r_2=3$	$r_2=4$
2	−0.485	0.625	—	—	—
3	−0.863	0.242	—	—	—
4	−1.130	0.178	0.850	—	—
5	−1.341	−0.084	0.597	—	—
6	−1.347	−0.286	0.380	1.133	—
7	−1.983	?	?	?	—
8	−1.532	?	?	?	1.406

We have at our disposal the work of Craig [19], [20], who showed how to construct the lattices E_6, E_8, Λ_{24} (Leech lattice) from the totally complex cyclotomic fields $K = \boldsymbol{Q}(e^{i2\pi/N})$ for $N = 9, 20, 39$. Applying his procedure we found D_4 (Schlafli lattice), K_{12} (Coxeter–Todd's lattice), and Λ_{16} (Barnes–Wall's lattice) from the 8th, 21st, and the 40th root of unity. These lattices are obtained by applying the canonical embedding to particular integral ideals of the above cyclotomic fields. The ideals are given in Table IV. The lattices we obtain are actually sublattices of $\sigma(O_K)$. This means that they have the same diversity $L = n/2$ of $\sigma(O_K)$, but a much higher fundamental gain compared to the lattices presented in Section V.

To illustrate the construction of the most famous lattice sphere packings, we need a few more results from algebraic number theory.

A. Ideals in the Ring of Integers

In the sequel, all given definitions and properties for ideals are true only in number fields and are not necessarily valid in an arbitrary field. For more theoretical details, the reader should consult [11]–[13].

Definition 10: Let K be a number field of degree n and O_K its ring of integers. An **ideal** I of O_K is a sub-$\boldsymbol{Z}$-module of O_K such that for every $a \in O_K$ and $b \in I$ we have $ab \in I$, briefly $aI \subset I$ and $bO_K \subset I$.

The sum and the product of two ideals I and J of O_K are also ideals of O_K and are defined by

$$I + J = \{x + y, \text{ where } x \in I \text{ and } y \in J\}$$
$$IJ = \left\{ \sum_i x_i y_i, \text{ where } x_i \in I \text{ and } y_i \in J \right\}.$$

Similarly, the intersection of two ideals is an ideal and we have the inclusions

$$IJ \subset I \cap J \subset I \subset I + J.$$

Definition 11: An ideal I of O_K is called **prime** (or **maximal**) if the quotient ring O_K/I is a field. I is called **principal** if $I = \alpha O_K$ for some algebraic integer α, in this case we also denote $I = (\alpha)$.

Result 9: Let I be a nonzero ideal of O_K. Then I is a module of maximal rank. The quotient ring O_K/I is finite and its cardinality is called the **norm** of the ideal I and denoted

$$N(I), N(I) = \text{Card}\,(O_K/I) = [O_K : I].$$

If $\omega_1, \omega_2, \cdots, \omega_n$ is an integral basis of O_K, we can write $O_K = \omega_1 \boldsymbol{Z} + \omega_2 \boldsymbol{Z} + \cdots + \omega_n \boldsymbol{Z}$. It simply means that the integral basis is a $\boldsymbol{Z}$-basis and that O_K is a module of maximal rank n. Let x be a nonzero element of I. The following relation $xO_K \subset I \subset O_K$ shows that I is included in a module of rank n and that I contains a module of rank n. Hence, I itself has the maximal rank n. It can be expressed as $I = \gamma_1 \boldsymbol{Z} + \gamma_2 \boldsymbol{Z} + \cdots + \gamma_n \boldsymbol{Z}$ where γ_i are elements of O_K. The proposition below follows:

Result 10: Any nonzero ideal I of O_K can be written as $I = \gamma_1 \boldsymbol{Z} + \gamma_2 \boldsymbol{Z} + \cdots + \gamma_n \boldsymbol{Z}$. The set $\{\gamma_i, i = 1 \cdots n\}$ is called a $\boldsymbol{Z}$-basis of I.

After applying the canonical embedding σ to the ideal I included in the ring O_K, we obtain the lattice $\Lambda_I = \sigma(I)$ of rank n included in $\Lambda = \sigma(O_K)$. As a consequence of the two above results, the generator matrix G_I of Λ_I is given by (17) at the bottom of this page.

Logically, we ask for the relation between the two matrices G and G_I. This can be found by comparing O_K and I as $\boldsymbol{Z}$-modules. Let T be the $n \times n$ matrix associated with the transition from the first basis to the second basis, i.e.

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = T \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Indeed, the γ_i's are algebraic integers and can be written as linear combinations of the ω_i's. $\gamma_i = \Sigma_{k=1}^{n} t_{ik}\omega_k$, where $t_{ik} \in \boldsymbol{Z}$. We deduce that $T = [t_{ij}]$ is an integer matrix. T is also known as the **integral matrix representation** of I. Furthermore, we can announce the following result:

Result 11: The generator matrix G_I of the lattice Λ_I can be obtained from the generator matrix G of the lattice Λ by applying the transition T between the $\boldsymbol{Z}$-bases of I and O_K, briefly $G_I = TG$.

This is derived directly from the formula $\gamma_i = \Sigma_{k=1}^{n} t_{ik}\omega_k$, which is also valid after taking the real part and the imaginary part of both sides

$$\sigma_j(\gamma_i) = \sum_{k=1}^{n} \sigma_j(t_{ik}\omega_k) = \sum_{k=1}^{n} t_{ik}\sigma_j(\omega_k).$$

$$G_I = \begin{pmatrix} \sigma_1(\gamma_1) & \cdots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \cdots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\gamma_n) & \cdots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix}. \quad (17)$$

The equality $G_I = TG$ allows us to write $\det G_I = \det T \times \det G$ which means that $\mathrm{vol}\,(\Lambda_I) = |\det T| \times \mathrm{vol}\,(\Lambda)$. The last equation can be used to compute the fundamental volume of Λ_I.

Result 12:

$$\mathrm{vol}\,(\Lambda_I) = N(I) \times 2^{-r_2} \times \sqrt{|d_K|}. \tag{18}$$

Proof: By definition $N(I)$ is equal to the cardinality of O_K/I. But O_K/I is isomorphic to the quotient Λ/Λ_I due to the canonical embedding σ. Thus they have the same cardinality (or same index as quotient groups). So we have $N(I) = |\Lambda/\Lambda_I|$. But the group partitioning [7], $\Lambda = \Lambda_I + [\Lambda/\Lambda_I]$, shows that a fundamental region of the sublattice Λ_I can be constructed as the disjoint union of $|\Lambda/\Lambda_I|$ copies of a fundamental region of Λ i.e.

$$\mathrm{vol}\,(\Lambda_I) = |\Lambda/\Lambda_I| \times \mathrm{vol}\,(\Lambda) = N(I) \times \mathrm{vol}\,(\Lambda).$$

Finally, (18) is obtained by combining $\mathrm{vol}\,(\Lambda_I) = N(I) \times \mathrm{vol}\,(\Lambda)$ and (13). Q.E.D.

Now we can relate T and $N(I)$ with $N(I) = |\det T|$, since

$$\mathrm{vol}\,(\Lambda_I) = N(I)\,\mathrm{vol}\,(\Lambda) = |\det T|\,\mathrm{vol}\,(\Lambda).$$

This is very useful especially when I is a principal ideal. In this case, the transition matrix is function of α and will be denoted $T = R(\alpha)$.

Result 13: Let $I = \alpha O_K$ be a principal ideal. The norm of I is equal to the absolute value of the algebraic norm of its generating element $N(I) = |N(\alpha)|$.

Proof: The $\boldsymbol{Z}$-basis of the principal ideal $I = \alpha O_K$ is the set $\{\alpha\omega_i, i = 1 \cdots n\}$. The transition equation becomes

$$\alpha \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = R(\alpha) \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}. \tag{19}$$

Recall that $T = R(\alpha)$ and $N(I) = |\det T|$. If we take all the conjugates of the above identity,

$$\sigma_k(\alpha)(\sigma_k(\omega_1), \sigma_k(\omega_2), \cdots, \sigma_k(\omega_n))' = R(\alpha)(\sigma_k(\omega_1), \sigma_k(\omega_2), \cdots, \sigma_k(\omega_n))'$$

for $k = 1, 2, \cdots, n$,where the prime indicates the transposition of the vector. We can write in a concise form

$$\Omega\,\mathrm{diag}(\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)) = R(\alpha)\Omega$$

where $\Omega = [\sigma_j(\omega_i)]$ for $i, j = 1, \cdots, n$. Taking the determinant we obtain $\det R(\alpha) = N(\alpha)$ and finally $N(I) = |\det R(\alpha)| = |N(\alpha)|$. Q.E.D.

Example 5: Let $K = \boldsymbol{Q}(\sqrt{5})$ and let θ be a primitive element with minimal polynomial $x^2 - x - 1$. Given $\alpha = \theta - 3 \in O_K$, we want to compute the integer transition matrix $T = R(\alpha) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Using (19) with $\omega_i = \theta^{i-1}$ and the identity $\theta^2 = \theta + 1$, derived from the minimal polynomial, we obtain

$$\begin{pmatrix} \theta - 3 \\ -2\theta + 1 \end{pmatrix} = \begin{pmatrix} a + b\theta \\ c + d\theta \end{pmatrix}$$

which gives $R(\alpha) = \left(\begin{smallmatrix} -3 & 1 \\ 1 & -2 \end{smallmatrix}\right)$. We now have

$$N(\theta - 3) = N(-5 + \sqrt{5}/2) = 5$$

which is equal to $\det R(\theta - 3)$. The generator matrix G_I of Λ_I, where $I = \alpha O_K$, is computed by

$$G_I = TG = R(\theta - 3)G = \begin{pmatrix} \dfrac{-5 + \sqrt{5}}{2} & \dfrac{-5 - \sqrt{5}}{2} \\ -\sqrt{5} & \sqrt{5} \end{pmatrix}$$

and (18) can be easily verified.

We have seen the $\boldsymbol{Z}$-basis representation of an ideal I. This representation was very practical to get properties for the associated lattice $\Lambda_I = \sigma(I)$. Equation (18) is very important and will guide us in the construction of Λ_I. We note also that the norm of the product of two ideals in O_K is equal to the product of the norms $N(IJ) = N(I)N(J)$. This result is closely related to (18). Sometimes when searching for an ideal of a given norm $N(I)$ to build Λ_I, we start from an ideal H such that $N(H) = cN(I)$ where c is an integer constant. Clearly, we are tempted to search for an ideal $H = IJ, c = N(J)$. Hence, we face the problem of factoring an ideal in the ring of integers. The factorization method for principal ideals is given in Result 16. Unfortunately, the factorization is a little bit difficult if we use the $\boldsymbol{Z}$-basis representation of the ideal. The following result shows a new representation of an ideal based on two elements of O_K.

Result 14: Let I be an ideal of O_K. For any nonzero element $\alpha \in I$ there exists an element $\beta \in I$ such that $I = \alpha O_K + \beta O_K$. α and β are called O_K-**generators** of I. The ideal is denoted $I = (\alpha, \beta)$.

The above result says that any ideal I in O_K can be expressed as the sum of two principal ideals. What about the $\boldsymbol{Z}$-basis of $I = \alpha O_K + \beta O_K$? This can be found if we notice that

$$I = \alpha\omega_1\boldsymbol{Z} + \cdots + \alpha\omega_n\boldsymbol{Z} + \beta\omega_1\boldsymbol{Z} + \cdots + \beta\omega_n\boldsymbol{Z}.$$

We obtain $2n$ $\boldsymbol{Z}$-generators of I. But the transition matrix T is defined only by n $\boldsymbol{Z}$-generators. So the difficulty is to determine a $\boldsymbol{Z}$-basis with n elements given a $\boldsymbol{Z}$-basis with $2n$ elements. This can be done by searching for the $n \times n$ integer matrix T whose rows span the same subgroup of $\boldsymbol{Z}^n$ generated by the rows of $R(\alpha)$ and $R(\beta)$.

Result 15: Every ideal I of O_K can be written in a unique way as

$$I = \prod_J J^{e_J}$$

the product being over a finite set of prime ideals J. The exponents e_J are positive integers.

Result 16: Let $K = \boldsymbol{Q}(\theta)$ be a number field, where θ is an algebraic integer, whose minimal polynomial is denoted $\mu(x)$. Let $f = [O_K : \boldsymbol{Z}[\theta]]$. Then for any prime p not dividing f one can obtain the factorization of the principal ideal $I = pO_K$ as follows. Let

$$\mu(x) = \prod_{i=1}^{g} \mu_i(x)^{e_i} \pmod p$$

TABLE IV
SOME KNOWN LATTICES FROM CYCLOTOMIC FIELDS

	$\mathbf{Q}(\theta)$	N	Ideals
$D_{4,2}$	θ^4+1	8	$(2,\theta+1)$
$E_{6,3}$	$\theta^6-\theta^3+1$	9	$(3,(\theta+1)^2)$
$E_{8,4}$	$\theta^8-\theta^6+\theta^4-\theta^2+1$	20	$(5,\theta-2)$
$K_{12,6}$	$\theta^{12}-\theta^{11}+\theta^9-\theta^8+$ $+\theta^6-\theta^4+\theta^3-\theta+1$	21	$(7,\theta+3)$
$\Lambda_{16,8}$	$\theta^{16}-\theta^{12}+\theta^8-\theta^4+1$	40	$(2,\theta^4+\theta^3+\theta^2+\theta+1)$ $(5,\theta^2+2)$
$\Lambda_{24,12}$	$\theta^{24}-\theta^{23}+\theta^{21}-\theta^{20}+\theta^{18}-\theta^{17}+\theta^{15}-\theta^{14}$ $+\theta^{12}-\theta^{10}+\theta^9-\theta^7+\theta^6-\theta^4+\theta^3-\theta+1$	39	$(3,\theta^3+\theta^2-1)$ $(3,\theta^3+\theta^2+\theta+1)$ $(13,\theta-3)$

be the decomposition of $\mu(x)$ into irreducible monic factors $\mu_i(x)$ in the ring of polynomials over GF(p), the Galois field of order p. Then

$$I = pO_K = \prod_{i=1}^{g} J_i^{e_i}$$

where $J_i = pO_K + \mu_i(\theta)O_K$.

Furthermore, the index $f_i = [O_K/J_i : \mathrm{GF}(p)]$ is equal to the degree of $\mu_i(x)$. We have

$$\deg(K) = n = \sum_{i=1}^{g} e_i f_i$$

and the norm of the prime ideal J_i is given by $N(J_i) = p^{f_i}$.

Let us check the norm of $I = pO_K$ in the factorization theorem. All the conjugates $\sigma_i(p)$ of p are equal to p because p is an integer. The algebraic norm of p is

$$N(p) = \prod_i \sigma_i(p) = p^n = N(I).$$

From the decomposition formula we see that

$$N(I) = \prod_{i=1}^{g} N(J_i^{e_i}) = \prod_{i=1}^{g} p^{e_i f_i} = p^n.$$

It is clear that the factorization of an ideal requires the factorization of a polynomial in a finite field (modulo p). The above algorithm will be used in the next subsection to decompose prime ideals while building the lattices of Table IV. Note that the ideals in Table IV are defined by two O_K-generators. The last two ideals (for Λ_{16} and Λ_{24}) are given as the product of two and three prime ideals, respectively.

B. Lattices from Cyclotomic Fields Ideals

In this section we assume that K is the cyclotomic field $K = \boldsymbol{Q}(\theta)$ where $\theta = e^{2i\pi/N}$ denotes a primitive Nth root of unity. Some well-known properties of cyclotomic fields are

1) The degree of K is $n = \phi(N)$, where ϕ is the Euler function.
2) The conjugates of θ are the θ^i with $\gcd(i,n) = 1$.
3) The ring of integers is $O_K = \boldsymbol{Z}[\theta]$ (the index f is 1).
4) The minimal polynomial of θ is

$$p(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

of degree $n = \phi(N)$, $\mu(i)$ is the Möbius function of the integer i.
5) The absolute discriminant of K is

$$d_K = (-1)^{n/2} N^n \Big/ \prod_{p|N} p^{n/(p-1)}.$$

Equation (18) is used to compute $N(I)$ given the lattice fundamental volume. The volume vol(Λ) is replaced by ρ^n/δ, where ρ is the packing radius and δ is the lattice center density [6]. The search for the rotated lattices of Table IV having dimension n and diversity $n/2$ goes through the following steps:

1) Calculate the minimal polynomial of $e^{i2\pi/N}$ which has degree $\phi(N)$.
2) Find all ideals I of O_K with integer norm

$$N(I) = \frac{2^{n/2}}{\sqrt{|d_K|}} \times \frac{\rho^n}{\delta}.$$

3) Using the transition matrix T of I compute the generator matrix $G_I = TG$ and evaluate the lattice parameters such as the center density and the kissing number. If they are equal to the parameters of $D_4, E_6, E_8, \Lambda_{12}, \Lambda_{16}$, or Λ_{24}, then we have obtained a rotated version of these lattices. In fact, these lattices are unique with such parameters.

This procedure was applied successfully to obtain a generator matrix for each one of the lattices in Table IV. The key operation is the factorization of prime ideals presented in Result 16.

We show as an example the new constructions of $D_{4,2}, K_{12,6}$ and $\Lambda_{16,8}$.

$D_{4,2}$

We first note that $\phi(8) = 4$ and that the other values of N giving $\phi(N) = 4$ do not result in the rotated version of D_4, whose center density is $1/8$. The minimal polynomial of $\theta = e^{i2\pi/8}$ is given in Table IV and the absolute discriminant of the field $K = \boldsymbol{Q}(\theta)$ is $d_K = 2^8$. The signature of K is $(0,2)$. Using (18) we can write

$$N(I) = \frac{2^{4/2}}{\sqrt{2^8}} \cdot \frac{\rho^4}{1/8} = 2^3 \cdot \rho^4$$

and for $N(I) = 2$ we may take $\rho = 1/\sqrt{2}$. The ideals I with norm 2 can be obtained from the factorization of the prime ideal (2), which has norm 2^4

$$(2) = (2, \theta+1)^4 = I^4.$$

Now I has the desired norm 2. The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix

representation of I

$$T = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density $0.125 = 1/8$ and kissing number 24 exactly like D_4. Since D_4 is the unique lattice with these parameters, we have constructed a rotated version of it with diversity equal to 2.

$K_{12,6}$

We first note that $\phi(21) = 12$ and that the other values of N giving $\phi(N) = 21$ do not result in the rotated version of K_{12}, whose center density is $1/27$. The minimal polynomial of $\theta = e^{i2\pi/12}$ is given in Table IV and the absolute discriminant of the field $K = \boldsymbol{Q}(\theta)$ is $d_K = 3^6 \cdot 7^{10}$. The signature of K is $(0, 6)$. Using (18) we can write

$$N(I) = \frac{2^{12/2}}{\sqrt{3^6 \cdot 7^{10}}} \times \frac{\rho^{12}}{1/27} = \frac{2^6 \cdot \rho^{12}}{7^5}$$

and for $N(I) = 7$ we may take $\rho = \sqrt{7}/\sqrt{2}$. The ideals I with such a norm can be obtained from the factorization of the ideal (7), having norm 7^{12}.

$$(7) = (7, \theta + 3)^6 (7, \theta - 2)^6 = I_1^6 I_2^6.$$

In fact, $N(I_1) = N(I_2) = 7$ so we may select $I = I_1$, which has the desired norm. The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix representation of I

$$T = \begin{pmatrix} 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density $1/27$ and kissing number 756 exactly like K_{12}. Since K_{12} is the unique lattice with these parameters, we have constructed a rotated version of it with diversity equal to 6.

$\Lambda_{16,8}$

We first note that $\phi(40) = 16$ and that the other values of N giving $\phi(N) = 16$ did not result in the rotated version of Λ_{16}, whose center density is $1/16$. The minimal polynomial of $\theta = e^{i2\pi/40}$ is given in Table IV and the absolute discriminant of the field $K = \boldsymbol{Q}(\theta)$ is $d_K = 2^{32} \cdot 5^{12}$. The signature of K is $(0, 8)$. Using (18) we can write

$$N(I) = \frac{2^{16/2}}{\sqrt{2^{32} \cdot 5^{12}}} \times \frac{\rho^{16}}{1/16} = \frac{\rho^{16}}{5^6 \cdot 2^4}$$

and for $N(I) = 2^4 \cdot 5^2$ we may take $\rho = \sqrt{2 \cdot 5}$. So we need to find the ideals I with such a norm. These can be obtained from the factorization of the ideals (2) and (5), having norms 2^{16} and 5^{16}, respectively.

$$(2) = (2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)^4 = I_1^4$$
$$(5) = (5, \theta^2 + 2)^4 (5, \theta^2 - 2)^4 = I_2^4 I_3^4$$

In fact

$$N(I_1) = 2^4, N(I_2) = 5^2, N(I_3) = 5^2$$

so we may select $I = I_1 I_2$ which has the desired norm

$$N(I) = N(I_1 I_2) = N(I_1) N(I_2) = 2^4 \cdot 5^2.$$

The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix representation of I and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density 0.0625 and kissing number 4320 exactly like Λ_{16}. Since Λ_{16} is the unique lattice with these parameters, what we have constructed is simply a rotated version of it with diversity equal to 8.

VII. Decoding and Practical Results

A. Decoding Algorithm

The lattices codes found in Sections V and VI, when used over the Gaussian channel, can be decoded using the algorithm shown in [21], [22]. This algorithm searches efficiently for all the lattice points inside a sphere of given radius $\sqrt{C}$ centered at the received vector and then outputs the closest one. It can be summarized as follow:

- *Input:* A received point $\boldsymbol{r}$ in the n-dimensional real space $\boldsymbol{R}^n$.
- *Output:* The lattice point $\boldsymbol{x}$ that minimizes $\Sigma_{i=1}^n |r_i - x_i|^2$.

1) Select a real positive constant C (the squared radius).
2) Enumerate all points in the n-dimensional sphere of radius $\sqrt{C}$ centered at $\boldsymbol{r}$.
3) Choose the closest point to $\boldsymbol{r}$.

We show how to adapt this lattice-decoding algorithm to the Rayleigh fading channel case. For maximum-likelihood decoding with perfect side information, the problem is to minimize the metric $m(\boldsymbol{x}|\boldsymbol{r}, \boldsymbol{\alpha})$ given in (2). Let G be the generator matrix of the lattice Λ and let us consider the lattice Λ_c with generator matrix

$$G_c = G \operatorname{diag}(\alpha_1, \cdots, \alpha_n).$$

We can imagine this new lattice Λ_c in a space where each component has been compressed or enlarged by a factor α_i. A point of Λ_c can be written as $\boldsymbol{u} = (u_1, \cdots, u_n) = (\alpha_1 x_1, \cdots, \alpha_n x_n)$. The metric to minimize is then

$$m(\boldsymbol{x}|\boldsymbol{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - u_i|^2.$$

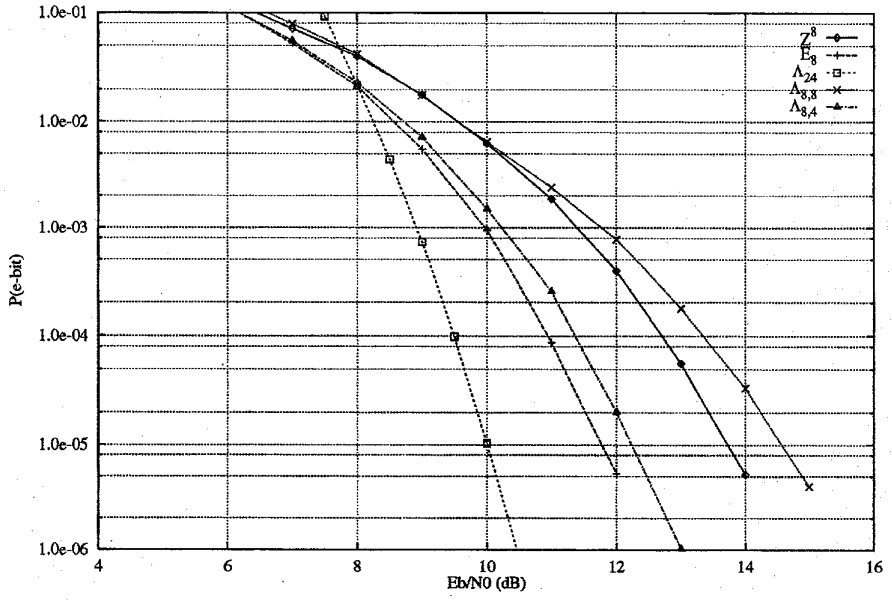

Fig. 2. Lattice constellations over the Gaussian channel ($\eta = 4$).

This means that we can simply apply the lattice decoding algorithm to the lattice Λ_c when the received point is $\boldsymbol{r}$. The decoded point $\hat{\boldsymbol{u}} \in \Lambda_c$ has the same integer components (in Z^n) as $\hat{\boldsymbol{x}} \in \Lambda$. The additional complexity required by this algorithm comes from the fact that for each received point we have a different compressed lattice Λ_c. So we need to compute a new Cholesky factorization of the Gram matrix for each Λ_c [11], [12]. We also need

$$G_c^{-1} = \text{diag}\,(1/\alpha_1, \cdots, 1/\alpha_n) G^{-1}$$

to find the components of the received vector but this only requires a vector–matrix multiplication since G^{-1} can be precomputed.

As discussed in [21], this decoding algorithm is maximum-likelihood only for an infinite lattice. When dealing with a finite constellation, with a given spectral efficiency, some care should be taken. In fact, the decoder may output a lattice point which is not part of the signal set. The constellations we have simulated are constituted by the points of the first shells of the lattice in order to obtain the minimal average energy per point. Since the decoding complexity increases with the search radius of the sphere, this is adaptively selected according to the fading coefficients so that we can always find at least a point of Λ_c inside the sphere. To optimize the decoder whenever the received point lays outside the outermost shell of the constellation we take its projection on this shell.

B. Results

We present some simulation results to illustrate and support some of the statements made throughout the paper. Due to the complexity of the decoding algorithm we have made simulations up to dimension eight while for higher dimensions we have plotted the upper bounds derived in the appendices. All built constellations have a spherical shape. All curves give the bit error probability as a function of E_b/N_0 for $\eta = 4$ bits/symbol. For convenience we will identify the lattice and the lattice constellation carved from it, with the same symbol.

Fig. 2 shows the performance of different lattice constellations over the Gaussian channel. Taking Z^8 as a reference we can make the following observations.

- E_8 only gains 2 dB at 10^{-5} although its asymptotic coding gain is 3 dB [6]. This draws the attention to the limitations of the asymptotic coding gain when used as parameter for practical values of the error probability.
- $\Lambda_{8,8}$, from the totally real field with minimal discriminant, loses (curve on the right of Z^8) 0.9 dB at 10^{-5} and asymptotically 1.5 dB (Table III), showing the weakness of these lattices over the Gaussian channel.
- $\Lambda_{8,4}$, from the totally complex field with minimal discriminant, gains 1.4 dB at 10^{-5} and is only 0.6 dB at 10^{-5} from E_8, the asymptotically eight-dimensional optimal lattice code for the Gaussian channel.

For comparison, Λ_{24} (at the most left) gains 3.7 dB over Z^8 at 10^{-5}. This curve is computed with (5) after adding 1.10 dB of shape gain.

Fig. 3 shows the performance over the Rayleigh fading channel of the rotated versions of the lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}$, the last two are upper bounds. As discussed in Section III, the slopes of the curves asymptotically correspond to the diversity. For these lattices we can see that this is already true for low bit error probabilities.

- At 10^{-3} the gain over Z^8 is about 17 dB and it exceeds 25 dB at 10^{-5}.
- $E_{8,4}$ outperforms $D_{4,2}$ with 10 dB at 10^{-5}.
- $K_{12,6}$ and $\Lambda_{16,8}$ curves (upper bounds) have been computed using (10) after neglecting high-diversity terms ($l \geq L + 1$).

Fig. 4 shows the performance over the Rayleigh fading channel of the lattice constellations from totally real algebraic

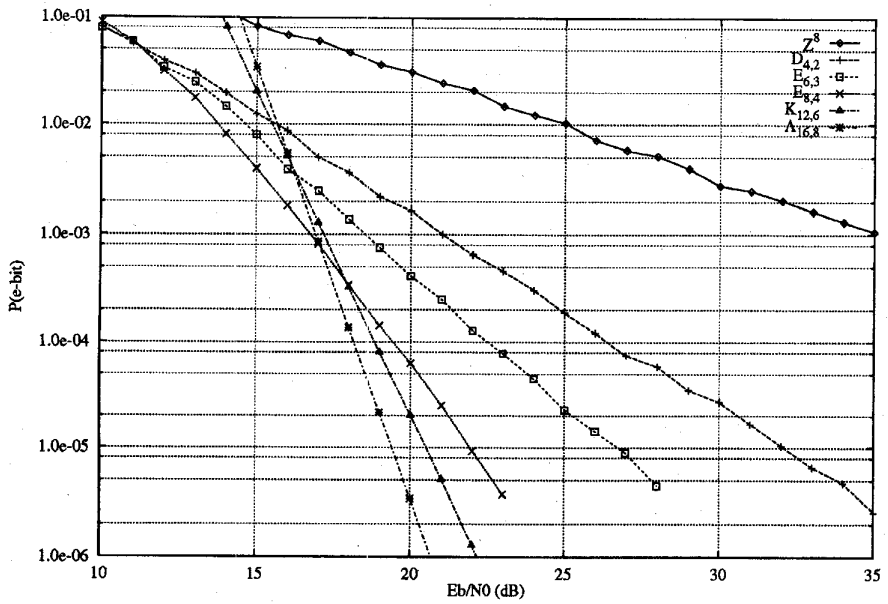

Fig. 3. Rotated famous lattice constellations over the Rayleigh fading channel ($\eta = 4$).

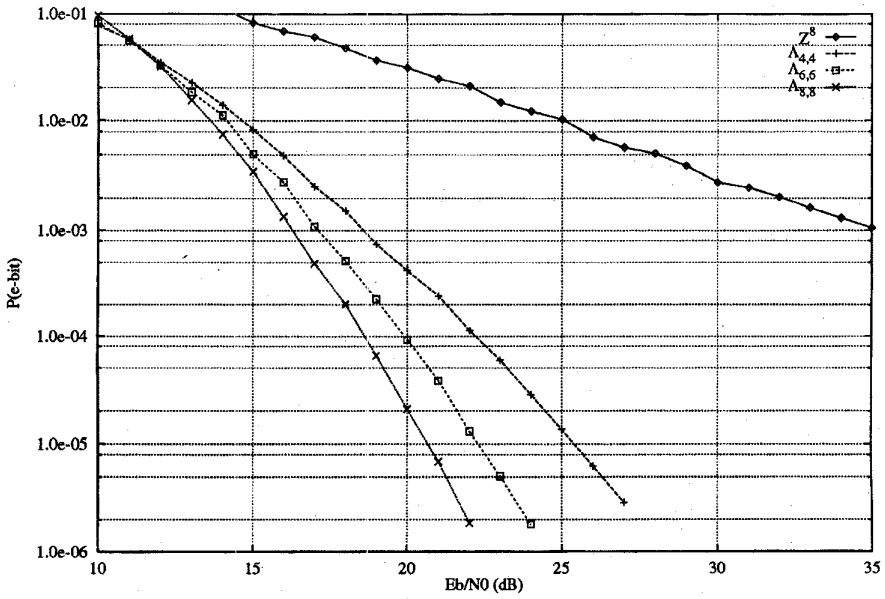

Fig. 4. Lattice constellations from totally real algebraic number fields of minimal discriminant over the Rayleigh fading channel ($\eta = 4$).

number fields. These lattices give a good performance over the fading channel but have negative asymptotic gains over the Gaussian channel. The gain of $\Lambda_{8,8}$ (compared to Z^8) on the Rayleigh channel is 19 dB at 10^{-3} and >25 at 10^{-5}. Although the theoretical diversities are comparatively higher, the actual slopes of the curves do not reach the asymptotic value in the range of interest. For example, $\Lambda_{8,8}$ curve at the most left shows a diversity of 4 instead of 8. An explanation of this fact comes from the high value of the product kissing number for these constellations.

Fig. 5 shows the performance over the Rayleigh fading channel of the lattice constellations from totally complex algebraic number fields. The curves achieve quite rapidly the slope corresponding to the diversity and their performance over the fading channel is very close to the one of the corresponding lattices in Fig. 4.

VIII. Conclusions

Two different approaches (Sections IV, V versus Section VI) have been used to study two families of lattices in order to achieve good performance over both Gaussian and Rayleigh channels, with high spectral efficiency.

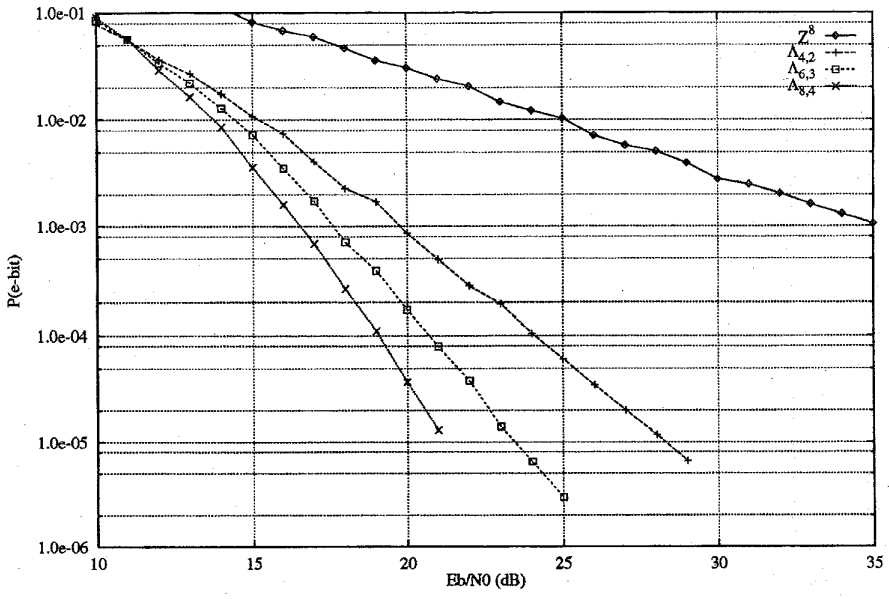

Fig. 5. Lattice constellations from totally complex algebraic number fields of minimal discriminant over the Rayleigh fading channel ($\eta = 4$).

The first family is generated by canonical embedding over the ring of integers of a number field. Among the lattices of this family, we especially gave importance to the classes of totally complex and totally real fields lattices. We found that totally real fields lattices (Λ_{real}) exhibit very good performance on Rayleigh channels with a maximal diversity of n. But they have a negative gain on Gaussian channels caused by their weak packing density. The totally complex fields lattices (Λ_{cplx}) are a compromise between diversity and packing density. They showed a positive gain on Gaussian channels and good performance on Rayleigh channels with a diversity of $n/2$.

The second family of lattices is generated by canonical embedding over special ideals in totally complex cyclotomic fields. This family includes versions of the famous lattice packings $D_4, E_6, E_8, K_{12}, \Lambda_{16}$, and Λ_{24}. These lattices act in a similar way as the $n/2$ diversity Λ_{cplx} lattices over the Rayleigh channel and thus can achieve a diversity from 2 through 12. Furthermore, these are the best lattices for the Gaussian channel.

The first important point in this conclusion is the fact that number fields with relatively small (or minimal) absolute discriminants are known only for degrees less or equal to 8. So the diversity of Λ_{real} cannot exceed 8, unless mathematicians find optimal fields with higher degree. On the contrary, the lattices of the second family are less limited in diversity; $\Lambda_{24,12}$ achieves a diversity of 12. Of course, we can think about building $\Lambda_{32,16}$ and $\Lambda_{64,32}$ to attain diversities 16 and 32, respectively. But we are limited by the ratio of the system's complexity over the practical gain. We cannot forget also that the study of the first family makes it possible for us to construct and understand the second family.

A second nonnegligible point to be mentioned concerns the practical aspects of lattice encoding/decoding. There exist no efficient algorithms for encoding and decoding the lattices presented in this paper, especially those of the first family. The universal decoding algorithm presented in the last section has a high complexity in terms of number of arithmetical operations. In fact, we are very pessimistic about finding a fast and a cheap decoding algorithm for the lattices of the first family. It is mainly too difficult to find a simple lattice (such as Z^n) containing these lattices and to make a group partitioning from which a simple encoding/decoding algorithm can be derived. On the contrary, we are very optimistic when it comes to elaborate efficient encoding/decoding algorithms for the $n/2$ diversity lattices of the second family viewed as rotated binary lattices.

Appendix I
Upper Bound on the AWGN Channel

In this Appendix we modify inequality (4) to express it as a function of E_b/N_0. We assume that the constellation S has a cubic shape centered at the origin and has volume $(2A)^n$. The components x_i of any point $\boldsymbol{x}$ in S satisfy the inequality $|x_i| \leq A$. The total number of points in S can be approximated by

$$M \approx \frac{(2A)^n}{\text{vol}\,(\Lambda)}$$

for sufficiently large M. We want to compute the average energy per point $E = E[\|\boldsymbol{x}\|^2]$ without specifying the particular lattice. Using a continuous approximation for the constellation points, we compute the second-order moment of the hypercube containing the constellation

$$E \approx \int_{[-A,A]^n} \|\boldsymbol{x}\|^2 \frac{d\boldsymbol{x}}{(2A)^n} = \int_{-A}^{A} \cdots \int_{-A}^{A} (x_1^2 + \cdots + x_n^2) \frac{dx_1 \cdots dx_n}{(2A)^n}.$$

The above integral is easily computed and gives $E = nA^2/3$.

Since

$$A^2 = \frac{M^{2/n}\,\mathrm{vol}\,(\Lambda)^{2/n}}{4} = \frac{2^{\eta}\,\mathrm{vol}\,(\Lambda)^{2/n}}{4}$$

the average energy per bit is

$$E_b = \frac{E}{n \times \eta} = \frac{A^2}{3\eta} = \frac{2^{\eta}\,\mathrm{vol}\,(\Lambda)^{2/n}}{12\eta}$$

and

$$\frac{d_{E\min}/2}{\sqrt{2N_0}} = \sqrt{\frac{d_{E\min}^2}{8N_0}} = \sqrt{\frac{3\eta}{2^{\eta+1}}\frac{E_b}{N_0}\frac{d_{E\min}^2}{\mathrm{vol}\,(\Lambda)^{2/n}}}.$$

This yields the upper bound (5) to the error probability for the AWGN channel.

Appendix II
Upper Bound on the Rayleigh Channel

In this Appendix we derive an upper bound for the pairwise point error probability $P(\boldsymbol{x} \rightarrow \boldsymbol{y})$ on the Rayleigh fading channel. The channel power gain is assumed normalized $E[\alpha_i^2] = 1$. As described in Section II, the components r_i of the received vector are given by $r_i = \alpha_i x_i + n_i$. The received point $\boldsymbol{r}$ is closer to $\boldsymbol{y}$ than to $\boldsymbol{x}$, if $m(\boldsymbol{y}|\boldsymbol{r}, \boldsymbol{\alpha}) \leq m(\boldsymbol{x}|\boldsymbol{r}, \boldsymbol{\alpha})$. The conditional pairwise error probability is given by

$$\begin{aligned}
P(\boldsymbol{x} \rightarrow \boldsymbol{y}|\boldsymbol{\alpha}) &= P\Bigg(\sum_{i=1}^{n} |r_i - \alpha_i y_i|^2 \\
&\qquad \leq \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 | \boldsymbol{x} \text{ transmitted}\Bigg) \\
&= P\left(\sum_{i=1}^{n} |\alpha_i(x_i - y_i) + n_i|^2 \leq \sum_{i=1}^{n} |n_i|^2\right) \\
&= P\Bigg(\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2 \\
&\qquad + 2\sum_{i=1}^{n} \alpha_i (x_i - y_i)\, n_i \leq 0\Bigg).
\end{aligned}$$

Now, let

$$\chi = \sum_{i=1}^{n} \alpha_i (x_i - y_i) n_i \cdot \chi$$

is a linear combination of Gaussian random variables (the n_i). Consequently, χ is Gaussian with zero mean and variance

$$\sigma_\chi^2 = N_0 \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2.$$

Let

$$A = 1/2 \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2$$

be a constant. We can write the conditional pairwise error probability in terms of χ and A

$$P(\boldsymbol{x} \rightarrow \boldsymbol{y}|\boldsymbol{\alpha}) = P(\chi \geq A) = Q(A/\sigma_\chi)$$

where

$$Q(x) = (2\pi)^{-1} \int_x^{\infty} \exp\left(-t^2/2\right) dt$$

is the Gaussian tail function. The Gaussian tail function can be upper-bounded [23] by an exponential $Q(x) \leq 1/2 \exp\left(-x^2/2\right)$. This bound is very tight already for $x \geq 3$. The conditional pairwise error probability becomes

$$\begin{aligned}
P(\boldsymbol{x} \rightarrow \boldsymbol{y}|\boldsymbol{\alpha}) &\leq \frac{1}{2} \exp\left(-\frac{A^2}{2\sigma_\chi^2}\right) \\
&= \frac{1}{2} \exp\left(-\frac{1}{8N_0} \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2\right).
\end{aligned}$$

The pairwise error probability $P(\boldsymbol{x} \rightarrow \boldsymbol{y})$ is computed by averaging $P(\boldsymbol{x} \rightarrow \boldsymbol{y}|\boldsymbol{\alpha})$ over the fading coefficients $\boldsymbol{\alpha}$

$$\begin{aligned}
P(\boldsymbol{x} \rightarrow \boldsymbol{y}) &= \int P(\boldsymbol{x} \rightarrow \boldsymbol{y}|\boldsymbol{\alpha}) \boldsymbol{p}(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} \\
&\leq \frac{1}{2} \int \exp\left(-\frac{1}{8N_0} \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2\right) \boldsymbol{p}(\boldsymbol{\alpha})\, d\boldsymbol{\alpha}.
\end{aligned}$$

The differential probability is

$$\boldsymbol{p}(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} = p(\alpha_1) \cdots p(\alpha_n)\, d\alpha_1 \cdots d\alpha_n$$

where $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ is the normalized Rayleigh distribution. Replacing in the last inequality we obtain

$$P(\boldsymbol{x} \rightarrow \boldsymbol{y}) \leq \tfrac{1}{2} \prod_{i=1}^{n} I_i$$

where

$$\begin{aligned}
I_i &= \int_0^{\infty} \exp\left(-\frac{1}{8N_0} \alpha_i^2 (x_i - y_i)^2\right) p(\alpha_i)\, d\alpha_i \\
&= \int_0^{\infty} 2\alpha_i \exp\left(-B_i \alpha_i^2\right) d\alpha_i
\end{aligned}$$

and $B_i = 1 + (x_i - y_i)^2/(8N_0)$. By simple calculations we obtain $I_i = 1/B_i$ and

$$P(\boldsymbol{x} \rightarrow \boldsymbol{y}) \leq \frac{1}{2} \prod_{i=1}^{n} \frac{1}{B_i}$$

which is (7) in Section III. This upper bound is sufficient to derive the optimization criteria for lattices on fading channels. It differs from the classical Chernoff bound by a factor $1/2$ and can be tightened by the use of Gaussian quadratic forms [5] which lead to a coefficient equal to $\binom{2L-1}{L}/4^L$ instead of $1/2$.

References

[1] 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.

[2] C. Schlegel and D. J. Costello, "Bandwidth efficient coding for fading channels: code construction and performance analysis," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 9, Dec. 1989.

[3] S. S. Pietrobon, R.H. Deng, A. Lafanechere, G. Ungerboeck, and D.J. Costello, "Trellis coded multidimensional phase modulation," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 63–89, Jan. 1990.

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

[5] C. Schlegel, "Trellis coded modulation on time-selective fading channels," *IEEE Trans. Commun.*, vol. 42, pp. 1617–1627, Feb./Mar./Apr. 1994.
[6] J. H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed. New York: Springer-Verlag, 1993.
[7] G. D. Forney, "Coset codes I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123–1151, 1988.
[8] K. Boullé and J. C. Belfiore, "Modulation scheme designed for the Rayleigh fading channel," preseented at CISS'92, Princeton, NJ, Mar. 1992.
[9] X. Giraud, "Constellations pour le canal à évanouissements," Ph.D. dissertation, E.N.S.T. Paris, France, May 1994.
[10] J. Boutros, "Constellations optimales par plongement canonique," *Mémoire de fin d'études*, E.N.S.T. Paris, France, June 1992.
[11] H. Cohen, *Computational Algebraic Number Theory*. New York: Springer-Verlag, 1993.
[12] M. E. Pohst, *Computational Algebraic Number Theory* (DMV Seminar, vol. 21). Basel, Switzerland: Birkhäuser Verlag, 1993.
[13] P. Samuel, *Algebraic Theory of Numbers*. Paris, France: Hermann, 1971.
[14] S. Lang, *Algebraic Number Fields*. Reading, MA: Addison-Wesley, 1971.
[15] H. Hasse, *Number Theory*. New York: Springer Verlag, 1980.
[16] J. Hunter, "The minimum discriminants of quintic fields," *Proc. Glasgow Math. Assoc.*, vol. 3, pp. 57–67, 1957.
[17] J. Liang and H. Zassenhaus, "The minimum discriminant of sixth degree totally complex algebraic number fields," *J. Number Theory*, vol. 9, pp. 16–35, Jan. 1977.
[18] F. Diaz y Diaz, "Petits discriminants des corps de nombres totalement imaginaires de degré 8," *J. Number Theory*, vol. 25, no. 1, pp. 34–52, Jan. 1987.
[19] M. Craig, "Extreme forms and cyclotomy," *Mathematika*, vol. 25, pp. 44–56, 1978.
[20] ——, "A cyclotomic construction for Leech's lattice," *Mathematika*, vol. 25, pp. 236–241, 1978.
[21] E. Viterbo and E Biglieri, "A universal lattice decoder," presented at the 14-ème Colloque GRETSI, Juan-les-Pins, France, Sept. 1993.
[22] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comp.*, vol. 44, pp. 463–471, 1985.
[23] S. Benedetto, E. Biglieri, and V. Castellani, *Digital Transmission Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1987.
[24] ANSI Asymmetric Digital Subscriber Line (ADSL) Working Draft Standard, T1E1.4/94-091R4, Sept. 1994.
[25] IEEE Working Group 802.11, P802.11-93/20b0, Update of Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, March 1994.
[26] K. Pahlavan and A.H. Levesque, *Wireless Information Networks*. New York: Wiley Interscience, 1995.