Algebraic Lattices Achieving the Capacity of the Ergodic Fading Channel

Antonio Campello
Dept. Communications et Electronique
Télécom ParisTech
Paris, France
campello@telecom-paristech.fr

Cong Ling
Department of Electrical
and Electronic Engineering
Imperial College London, U.K.
cling@ieee.org

Jean-Claude Belfiore
Mathematical and Algorithmic Sciences Lab
France Research Center
Huawei Technologies
belfiore@telecom-paristech.fr

***Abstract*—In this work we show that algebraic lattices constructed from error-correcting codes achieve the ergodic capacity of the fading channel. The main ingredients for our construction are a generalized version of the Minkowski-Hlawka theorem and shaping techniques based on the lattice Gaussian distribution. The structure of the ring of integers in a number field plays an important role in the proposed construction. In the case of independent and identically distributed fadings, the lattices considered exhibit full diversity and an exponential decay of the probability of error with respect to the blocklength.**

I. Introduction

Lattice codes provide structured solutions for communication in the presence of Gaussian noise. They have been proved to be capacity achieving on the AWGN channel [1] and admit efficient implementations based on error correcting codes, such as polar [2] and LDPC codes [3].

In contrast, a great part of the literature on lattices for the fading channel mainly concerns modulation aspects such as the diversity and the product distance [4]. Signal constellations with some additional algebraic structure were first investigated in the context of the Rayleigh fast fading channel [5] and are well-known to exhibit very good practical performance. For instance, they achieve full modulation diversity i.e., for a given blocklength n, their probability of error has optimal scaling with the signal-to-noise ratio $O(\text{SNR}^{-n})$.

More recently, capacity approaching lattices have been considered for the fading channel in [6], [7], [8]. Random arguments are used in [6] to prove that lattices achieve the "infinite capacity" (or the Poltyrev limit) of the fast fading channel under some regularity conditions. If applied to usual mod-p lattices [9], the constellations exhibit diversity *one*.

In another direction, the work [8] constructs *deterministic* lattice codes based on algebraic number theory that operate at a certain gap to capacity; strong connections between the minimum product distance and their attainable rates are established. However, to our knowledge, the question of whether lattices with algebraic (multiplicative) structure can operate on the ergodic fading channel with rates up to the capacity and vanishing probability of error was still open.

In this work we answer this question in the affirmative by showing that algebraic lattices codes achieve the capacity in the ergodic fading channel. The constructions considered here enjoy some desirable properties of good modulation schemes (in particular full diversity), while are *provably* capacity-achieving. In the same flavor of [8], some ingredients of our construction leverage from the Geometry of Numbers. The main techniques used here are:

- A Minkowski-Hlawka theorem for a generalized (algebraic) version of Construction A lattices (Theorem 1). This Construction A was first proposed in [10], but its asymptotic goodness was up to now unknown.
- Properties of the group of units in the ring of integers (lemmas 1 and 2).
- The lattice Gaussian distribution for shaping the constellation (Section V).

Comparison with Previous Results

The work [6] presents the analysis of infinite constellations for the fading channel. Under the condition that the fading coefficients are identically distributed and obey a regularity condition (satisfied by many practical distributions), it is shown that random lattices can achieve the Poltyrev limit of the fast fading channel, with vanishing error probability. The error probability decays with quadratic order $O(1/n^2)$ with respect to the dimension.

Algebraic lattices (with full diversity) based on a tower of number fields with bounded discriminant have been shown to achieve a constant gap to capacity of the ergodic fading channel in [8]. For the real Rayleigh fading case, the gap is greater than 3.97 bits per channel uses and can be reduced to ≈ 1.33 at best, under optimistic assumptions.

Here we bridge the gap between random and algebraic constructions by considering *random algebraic lattices* for the fading channel. While the algebraic structure allows the construction of lattices with full diversity, the random arguments simplify the analysis and eliminate the gap to capacity. For iid fadings, the error probability obtained decays exponentially with the blocklength.

II. Initial Definitions

A. Channel Model

We consider the channel described by the equation

$$y_i = h_i x_i + z_i \tag{1}$$

for $i = 1, 2, \ldots$, where z_i is a Gaussian noise $\sim \mathcal{N}(0, \sigma^2)$ and $\{h_i\}$ is a stationary ergodic random process with $E[h_i^2] = 1$. The input values have average power lesser or equal than P. Let $\text{SNR} \triangleq P/\sigma^2$. The capacity of this channel is [11][1]

$$C = E\left[\frac{1}{2}\log\left(1 + h^2\text{SNR}\right)\right] \text{ nats/channel use}$$

and it is known to be achievable with random codes. A special case is when the fading coefficients are independent and identically distributed. Distributions widely used in practice are the Rayleigh distribution and its generalization, the Nakagami distribution.

B. Lattices

A (full rank) lattice $\Lambda \subset \mathbb{R}^n$ has the form

$$\Lambda = \{B\mathbf{u} : \mathbf{u} \in \mathbb{Z}^n\}, \tag{2}$$

where $B \in \mathbb{R}^{n\times n}$ is a full rank matrix. The *Voronoi region* of a point $\mathbf{x} \in \Lambda$ is defined as

$$\mathcal{V}_\Lambda(\mathbf{x}) \triangleq \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{y}\| \leq \|\bar{\mathbf{x}} - \mathbf{y}\| \text{ for all } \bar{\mathbf{x}} \in \Lambda\}.$$

We write $\mathcal{V}_\Lambda = \mathcal{V}_\Lambda(\mathbf{0})$. The volume of Λ is defined as the volume of its Voronoi region and denoted by $V(\Lambda)$. It follows that $V(\Lambda) = |\det B|$. Given $\sigma > 0$, the *volume-to-noise ratio* (VNR) of a lattice is defined as

$$\gamma_\Lambda(\sigma) \triangleq \frac{V(\Lambda)^{2/n}}{\sigma^2}.$$

1) The Lattice Gaussian Distribution: We denote the Gaussian distribution of variance σ^2 as

$$f_\sigma(\mathbf{x}) \triangleq \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}},$$

for all $\mathbf{x} \in \mathbb{R}^n$. The *discrete Gaussian distribution* is the following discrete distribution taking values in $\lambda \in \Lambda$ with probability

$$D_{\Lambda,\sigma}(\lambda) \triangleq \frac{f_\sigma(\lambda)}{\sum_{\mathbf{x}\in\Lambda} f_\sigma(\mathbf{x})}$$

For a lattice Λ and for a parameter σ, an important quantity is the flatness factor, given by

$$\epsilon_\Lambda(\sigma) \triangleq \max_{\mathbf{x}\in\mathcal{V}_\Lambda} |V(\Lambda) f_{\sigma,\Lambda}(\mathbf{x}) - 1|. \tag{3}$$

2) Product distance: The *product distance* of a lattice Λ is defined as

$$d_{\text{prod}}(\Lambda) \triangleq \min_{(x_1,\ldots,x_n)\in\Lambda\setminus\{0\}} \prod_{i=1}^{n} |x_1 \ldots x_n| \tag{4}$$

If $d_{\text{prod}}(\Lambda) > 0$, we say that Λ has *full diversity*. The error probability of a constellation chosen from a lattice with full diversity scales with order $O(\text{SNR}^{-n})$ [5], which motivates the terminology.

[1]All logarithms in this paper are with respect to base e

3) The Minkowski-Hlawka Theorem: An important element to show the existence of "good" lattices (with respect to various measures of goodness) is the *Minkowski-Hlawka Theorem*. Minkowski-Hlawka ensembles are families of lattices that satisfy a certain "mean-value theorem", as formalized next.

Definition 1. *An infinite ensemble $\mathbb{L}$ of lattices of volume V is said to be Minkowski-Hlawka (or MH) if for any integrable function $f : \mathbb{R}^n \to \mathbb{R}$ vanishing outside a bounded set, we have*

$$E_{\mathbb{L}}\left[\sum_{\mathbf{x}\in\Lambda\setminus\{0\}} f(\mathbf{x})\right] = V^{-1}\int_{\mathbb{R}^n} f(\mathbf{x})d\mathbf{x}. \tag{5}$$

Several MH ensembles were proposed in the Geometry of Numbers. A particularly useful construction was exhibited in [9], who showed an ensembles of lattices based on Construction A from codes over the field $\mathbb{F}_p$ are asymptotically MH ensembles, as the alphabet size goes to infinity.

III. Construction A

We now describe the algebraic Construction A proposed in [10]. We recall some main definitions and results, but assume some basic familiarity with Algebraic Number Theory.

Let $K/\mathbb{Q}$ be a field extension of degree $[K : \mathbb{Q}] = n$. There are $\sigma_1, \ldots, \sigma_n$ homomorphisms from K to $\mathbb{C}$ that fix $\mathbb{Q}$. We assume that $K/\mathbb{Q}$ is *totally real*, i.e., the image of the homomorphisms (called the *embeddings*) is in $\mathbb{R}$. We further assume that the extension is Galois, in which case $\sigma_i(K) = K$ for all i, and that the embeddings form an Abelian group under composition. Let $\mathcal{O}_K$ be the *ring of integers* of K, i.e., the elements in K that are the root of a monic polynomial with coefficients in $\mathbb{Z}$. It follows that $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank n. Consider the application $\psi : K \to \mathbb{R}^n$, often referred to as *the canonical embedding*:

$$\psi(x) = (\sigma_1(x), \ldots, \sigma_n(x)). \tag{6}$$

The image of $\mathcal{O}_K$ by ψ is a full rank lattice which we denote by $\Lambda_K \triangleq \psi(\mathcal{O}_K) \subset \mathbb{R}^n$. The volume squared of this lattice is referred to as the *discriminant* of K, and denoted by Δ_K.

Consider a prime p that splits completely i.e., $p\mathcal{O}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_n$, where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$. Let $\mathfrak{p} = \mathfrak{p}_i$ for some i. There exists an isomorphism $\phi : \mathcal{O}_K/\mathfrak{p} \to \mathbb{F}_p$. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ denote the projection operator. Consider the reduction mapping $\rho : \Lambda_K \to \mathbb{F}_p^n$ given by

$$\rho(\psi(x)) = (\phi \circ \pi)(\psi(x)), \tag{7}$$

where $(\phi \circ \pi)$ is applied component-wise in the canonical embedding. Let $\mathcal{C} \subset \mathbb{F}_p^n$ be a linear code with dimension k (or a code with parameters (n, k, p)). The Construction A lattice associated to $\mathcal{C}$ is defined as

$$\Lambda_K(\mathcal{C}) \triangleq \rho^{-1}(\mathcal{C}).$$

The properties of $\Lambda_K(\mathcal{C})$ are studied in [10]. First of all $\Lambda_K(\mathcal{C})$ is a full rank lattice and $\Lambda_K(\{0\}) = \phi(p\mathcal{O}_K)$ is a sublattice with index $|\mathcal{C}| = p^k$. In fact the quotient

$$\Lambda_K(\mathcal{C})/p\Lambda_K \simeq \mathcal{C}, \tag{8}$$

from where we can deduce that $V(\Lambda_K(\mathcal{C})) = p^{n-k}\sqrt{\Delta_K}$. It is further shown that $\Lambda_K(\mathcal{C})$ has full diversity and its product distance is bounded in terms of the Hamming distances of $\mathcal{C}$.

Example 1. *Let $\mathbb{Q}[\sqrt{13}]$ be the quadratic field with ring of integers $\mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{13}}{2}$ and $\bar{\alpha} = \frac{1-\sqrt{13}}{2}$. The two embeddings are determined by $\sigma_1(\sqrt{13}) = \sqrt{13}$ and $\sigma_2(\sqrt{13}) = -\sqrt{13}$. The prime $3 = -\alpha\bar{\alpha}$ splits and the ideal $\mathfrak{p} = \alpha\mathbb{Z}[\alpha]$ is such that $\mathbb{Z}[\alpha]/\mathfrak{p} \sim \mathbb{F}_3$. We can now identify the set of representatives for the quotient $\mathbb{Z}[\alpha]/3\mathbb{Z}[\alpha]$ with elements in $\mathbb{F}_3^2$, as in Figure 1. The pre-image by ρ of a code spreads its corresponding representatives in the plane.*

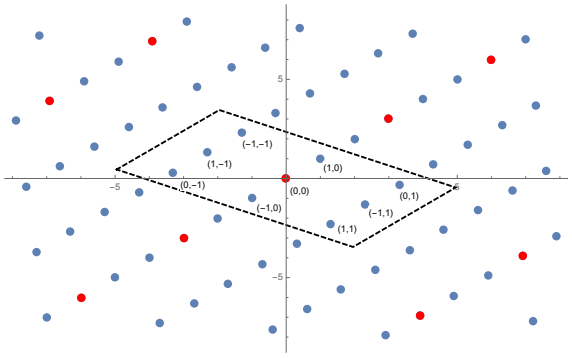

Fig. 1. Modulo $\mathfrak{p}$ operation

A. Asymptotic Goodness

Let $\beta > 0$ be a constant and $\alpha = (\beta^{1/n} p^{1-k/n} \Delta_K^{1/2n})^{-1}$ a normalization factor. Consider the ensemble of all lattices from generalized Construction A, normalized to volume $1/\beta$

$$\mathbb{L}_{K,n,k,p,\beta} = \{\alpha\Lambda_K(\mathcal{C}) : \mathcal{C} \text{ is an } (n,k,p) \text{ code } \}. \quad (9)$$

Using the machinery developed by [9], we can establish the following

Theorem 1. *Let f be a function with bounded support.*

$$\lim_{p\to\infty} E_{\mathbb{L}_{K,n,k,p,\beta}} \left[\sum_{\mathbf{x}\in\Lambda(\mathcal{C})\setminus\{\mathbf{0}\}} f(\mathbf{x}) \right] = \beta \int_{\mathbb{R}^n} f(\mathbf{x}) d\mathbf{x}, \quad (10)$$

where the expectation is with respect to the uniform distribution on $\mathbb{L}_{K,n,k,p,\beta}$.

Proof. First of all, we have to make sure that "$p \to \infty$" makes sense. This is a consequence of [12, Cor. 13.6 p. 547], which establishes the density of prime ideals in a Number Field; in particular there are infinitely many primes that split.

Let $\mathcal{C}_{n,k,p}$ be the set of all codes with parameters (n,k,p). It is proven in [9] that, for any function $g : \mathbb{F}_p^n \to \mathbb{R}$

$$\frac{1}{|C_{n,k,p}|} \sum_{\mathcal{C}\in\mathcal{C}_{n,k,p}} \sum_{\mathbf{c}\in\mathcal{C}\setminus\{0\}} g(\mathbf{c}) = \frac{p^k-1}{p^n-1} \sum_{\mathbf{v}\in\mathbb{F}_p^n\setminus\{0\}} g(\mathbf{v}). \quad (11)$$

The left-hand side of (10) reads

$$\frac{1}{|\mathcal{C}_{n,k,p}|} \sum_{\mathcal{C}\in\mathcal{C}_{n,k,p}} \sum_{x\in\alpha\Lambda_K(\mathcal{C})\setminus\{0\}} f(x) =$$
$$\frac{1}{|\mathcal{C}_{n,k,p}|} \sum_{\mathcal{C}\in\mathcal{C}_{n,k,p}} \left(\sum_{\substack{x\in\alpha\Lambda_K(\mathcal{C})\setminus\{0\} \\ \rho(\mathbf{x}/\alpha)=0}} f(x) + \sum_{\substack{x\in\alpha\Lambda_K(\mathcal{C})\setminus\{0\} \\ \rho(\mathbf{x}/\alpha)\neq 0}} f(x) \right). \quad (12)$$

Now if $\rho(\mathbf{x}/\alpha) = 0$, $\mathbf{x} = \alpha p\psi(\mathbf{o})$, where $\mathbf{o} \in \mathcal{O}_K\setminus\{0\}$. Since $p\alpha \to \infty$ as $p \to \infty$ and f has bounded support, for sufficiently large p, the last sum becomes:

$$\frac{1}{|\mathcal{C}_{n,k,p}|} \sum_{\mathcal{C}\in\mathcal{C}_{n,k,p}} \sum_{\substack{x\in\alpha\Lambda_K(\mathcal{C})\setminus\{0\} \\ \rho(\mathbf{x}/\alpha)\neq 0}} f(x) = \frac{p^k-1}{p^n-1} \sum_{x\in\Lambda_K\setminus\{0\}} f(\alpha x)$$
$$\to \beta \int_{\mathbb{R}^n} f(\mathbf{x}) d\mathbf{x} \text{ as } p \to \infty$$

□

Remark 1. *The role of the discriminant of the Number Field K is implicit in the proof of Theorem 1. Asymptotically, as long as K is fixed and $p \to \infty$ the theorem holds with no restrictions on Δ_K. However, if Δ_K is too large, the alphabet size will need to increase too much.*

For instance, let $f = \mathbb{1}_{\mathcal{B}(r)}$ be the indicator function of a ball. Then for the condition $\mathbb{1}_{\mathcal{B}(r)}(x) = 0$ to hold, we need $\alpha p > r$, or $p > (\beta^{1/n} r \Delta_K^{1/n})^{1/\eta}$, where $\eta = k/n$ is the rate of the underlying codes. To this respect, having a number field of small discriminant is desirable.

B. Invariance by Units

The set of all invertible elements in a number field, denoted by $\mathcal{O}_K^*$, forms a group under multiplication called the *group of units*. If $K = \mathbb{Q}$, the only units in $\mathcal{O}_K$ are $\{-1, 1\}$, however for higher degree extensions the group of units is much richer. In Example 1, $\mathcal{O}_K^*$ corresponds to all numbers of the form $\pm(\alpha+1)^k$, where $k \in \mathbb{Z}$. An element $u \in \mathcal{O}_K$ is a unit if and only if $\sigma_1(u)\dots\sigma_n(u) = \pm 1$.

The following property shows the invariance of the ensemble under multiplication by units. Denote by $*$ the Hadamard (or componentwise) product between two vectors.

Lemma 1. *If $u \in \mathcal{O}_K^*$, then $\psi(u) * \Lambda_K(\mathcal{C}_1) = \Lambda_K(\mathcal{C}_2)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same dimension.*

Proof. It suffices to show that $\psi(u) * \Lambda_K(\mathcal{C}_1) \subset \Lambda_K(\mathcal{C}_2)$, for some $\mathcal{C}_1$ and $\mathcal{C}_2$ of same rank, since both lattices have same volume due to the fact that $\sigma_1(u)\dots\sigma_n(u) = \pm 1$. Let $\mathbf{y} = \psi(u) * \lambda$, $\lambda = \psi(x) \in \Lambda_K(\mathcal{C}_1)$. Then

$$\rho(\psi(u) * \lambda) = (\phi \circ \pi)(\psi(u)) * (\phi \circ \pi)(\psi(x)) = \mathbf{a} * \mathbf{c},$$

where $\mathbf{c}$ is a codeword. It follows that $\mathbf{y} \in \Lambda_K(\mathbf{a} * \mathcal{C}_1)$. Now, since no coordinate of $\mathbf{a}$ is zero, multiplication by $\mathbf{a}$ does not affect the rank of $\mathcal{C}_1$, which finishes the proof. □

Remark 2. *In the previous lemma, $\mathcal{C}_1$ can be obtained from $\mathcal{C}_2$ by an equivalence of the Hamming Metric.*

From Lemma 1 the mapping $t_{\mathbf{u}} : \mathbb{L}_{K,n,k,p} \to \mathbb{L}_{K,n,k,p}$ given by $t_{\mathbf{u}}(\Lambda) = \psi(u) * \Lambda$ is a bijection of the ensemble. This property is useful to handle deep fadings, when combined with the following lemma:

Lemma 2 (Thm. 1, [13])**.** *Let $\mathbf{H} = diag(h_1, \ldots, h_n)$ be a channel matrix and let $\tilde{\mathbf{H}} = \mathbf{H}/\det(\mathbf{H}\mathbf{H}^{tr})^{1/2n}$. There exists a unit $u \in \mathcal{O}_K^*$ such that $\tilde{\mathbf{H}} = \mathbf{E}_{\mathbf{H}}\mathbf{U}$, where $\mathbf{U} = diag(\sigma_1(u), \ldots, \sigma_n(u))$ and*

$$\left\|\mathbf{E}_{\mathbf{H}}^{-1}\right\| \leq C_n$$

for a constant C_n that does not depend on $\mathbf{H}$.

An explicit bound on C_n is exhibited in [13], namely

$$C_n \leq \sqrt{n} e^{(n-1)\left(\frac{R_K}{\mathcal{V}_{n-1}}\right)^{1/(n-1)}},$$

where R_K is a parameter associated to K and $\mathcal{V}_{n-1}$ is the volume of an Euclidean unit sphere in $\mathbb{R}^{n-1}$.

IV. Infinite Lattice Constellations

The dispersion and the Poltyrev limit of infinite constellations for the stationary ergodic fading channel was analyzed in [6]. In this case, $\{h_i\}$ is a random process (not necessarily iid) for which $\mu = E[\log|h|]$ exists and

$$\lim_{n\to\infty} P\left(\left|\frac{1}{n}\sum_{i=1}^{n}\log|h_i| - \mu\right| > \varepsilon\right) = 0, \tag{13}$$

for any positive $\varepsilon > 0$. Corollary 4.1 of [6] implies that the smallest possible VNR for a sequence of lattices to have vanishing error probability is

$$\gamma^* = e^{-2\mu}2\pi e. \tag{14}$$

Let $P_e(\Lambda)$ be the probability of error of an infinite lattice scheme in a fading channel. In view of this result we can define fading-good lattices.

Definition 2. *A sequence Λ_n of lattices with increasing dimension is good for the ergodic fading channel if for all VNR $\gamma_\Lambda(\sigma) > e^{-2\mu}2\pi e$, $P_e(\Lambda) \to 0$ as $n \to \infty$.*

It was proven in [6], for iid fading processes under some regularity conditions, that there exists a sequence of fading-good lattices with $P_e(\Lambda) = O(1/n^2)$. The proof only requires an MH ensemble, and hence an immediate corollary of Theorem 1 is that Generalized Construction A lattices as in (10) are also fading good. We provide next a different approach that explores the algebraic structure and obtains an exponential decay of $P_e(\Lambda)$ with respect to n in iid fading channels.

Theorem 2. *There exists a sequence of ergodic fading-good lattices from Generalized Construction A* (10)*.*

Proof. Consider the received vector $\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z}$. Let $\Delta = |h_1 \ldots h_n|^{1/n}$ and let $\mathcal{S}$ be a ball of radius $(\Delta/e^{\mu-\delta})\sqrt{n(\sigma^2+\varepsilon)}$, for δ and ε sufficiently small. Consider a decoder that assigns $\hat{\mathbf{x}} = \tilde{\mathbf{x}}$ if $\mathbf{y}$ can be written in a unique way as $\mathbf{y} = \mathbf{H}\tilde{\mathbf{x}} + \mathbf{z}$, with $\tilde{\mathbf{x}} \in \Lambda, \mathbf{z} \in \mathcal{S}$, and "error" otherwise (in Loeliger's terminology [9] an ambiguity). For a set $\mathcal{M} \subset \mathbb{R}^n$, let

$$N_{\mathcal{M}}(\Lambda) \triangleq |(\Lambda \setminus \{0\}) \cap \mathcal{M}|.$$

We upper bound the probability of error as

$$P_e(\Lambda|\mathbf{H}) \leq P(\mathbf{z} \notin \mathcal{S}|\mathbf{H}) + P(N_{\mathbf{z}-\mathbf{S}}(\mathbf{H}\Lambda) \geq 1 | \mathbf{z} \in \mathcal{S}, \mathbf{H}),$$

and therefore

$$P_e(\Lambda) \leq E_{\mathbf{H}}\left[P(\mathbf{z} \notin \mathcal{S})\right] + E_{\mathbf{H}}\left[P(N_{\mathbf{z}-\mathbf{S}}(\mathbf{H}\Lambda) \geq 1 | \mathbf{z} \in \mathcal{S})\right]. \tag{15}$$

The first term does not depend on the chosen lattice and vanishes as $n \to \infty$. It can be bounded as

$$\begin{aligned} P(\mathbf{z} \notin \mathcal{S}) &\leq P(\mathbf{z} \notin \mathcal{S} | \Delta > e^{\mu-\delta}) + P(\Delta < e^{\mu-\delta}) \\ &\leq P(\mathbf{z} \notin \mathcal{B}_{\sqrt{n(\sigma^2+\varepsilon)}}) + P(\Delta < e^{\mu-\delta}). \end{aligned} \tag{16}$$

The second term in the right-hand side of (15) can be upper bounded by

$$\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} N_{\mathbf{z}-\mathbf{S}}(\mathbf{H}\Lambda) f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z}. \tag{17}$$

Let $\mathbb{L} = \mathbb{L}_{K,n,k,p}$ be the ensemble of Generalized Construction A lattices and consider the decomposition $\mathbf{H} = \Delta\mathbf{E}_{\mathbf{H}}\mathbf{U}_{\mathbf{H}}$, as in Lemma 2. Let $f_h(\mathbf{h})$ be the pdf of the joint distribution of $(h_1, \ldots, h_n)$. Taking the average over the ensemble (notice that at this point, for finite p, the ensemble is finite and we can commute integrals and sums):

$$\begin{aligned} &E_{\mathbb{L}}\left[\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} N_{\mathbf{z}-\mathbf{S}}(\mathbf{H}\Lambda) f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z}\right] = \\ &\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} E_{\mathbb{L}}\left[N_{\mathbf{z}-\mathbf{S}}(\mathbf{H}\Lambda)\right] f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z} \overset{(a)}{=} \\ &\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} E_{\mathbb{L}}\left[N_{\mathbf{z}-\mathbf{S}}(\Delta\mathbf{E}_{\mathbf{H}}\Lambda)\right] f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z} = \\ &E_{\mathbb{L}}\left[\sum_{\mathbf{x}\in\Lambda\setminus\{0\}}\int_{\mathbb{R}^n}\int_{\mathbb{R}^n} \mathbb{1}_{\Delta^{-1}\mathbf{E}_{\mathbf{H}}^{-1}(\mathbf{z}-\mathbf{S})}(\mathbf{x}) f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z}\right], \end{aligned}$$

where (a) is due to the fact that multiplication by unit is a bijection of the ensemble. Now take

$$g(\mathbf{x}) = \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} \mathbb{1}_{\Delta^{-1}\mathbf{E}_{\mathbf{H}}^{-1}(\mathbf{z}-\mathbf{S})}(\mathbf{x}) f_{\mathbf{z}|\mathcal{S}}(z) f_h(\mathbf{h}) d\mathbf{h} d\mathbf{z}. \tag{18}$$

We argue that $g(\mathbf{x})$ has bounded support. In effect, if $\mathbf{x}$ is such that $\|\mathbf{x}\| > 2(C_n/e^{\mu-\delta})\sqrt{n(\sigma^2+\varepsilon)}$, then $\|\Delta\mathbf{E}_{\mathbf{H}}\mathbf{x}\| > 2(\Delta/e^{\mu-\delta})\sqrt{n(\sigma^2+\epsilon)}$, which implies that $\mathbb{1}_{\Delta^{-1}\mathbf{E}_{\mathbf{H}}^{-1}(z-S)}(\mathbf{x}) = 0$ and $g(\mathbf{x}) = 0$. Therefore Theorem 1 applies. When $p \to \infty$, we get

$$\lim_{p\to\infty} E_{\mathbb{L}}\left[\sum_{\mathbf{x}\in\Lambda\setminus\{0\}} g(\mathbf{x})\right] = e^{-n(\mu-\delta)}\beta \text{ vol}\,\mathcal{B}_{\sqrt{n(\sigma^2+\varepsilon)}}. \tag{19}$$

Therefore, there exists a sequence of lattices in the random ensemble such that $P_e(\Lambda)$ decays to zero, as long as the VNR is greater γ^* (Equation (14)). □

Under the additional assumption that the random process converges exponentially to its mean, we obtain the following direct corollary

Corollary 1. *If for any sufficiently small $\varepsilon > 0$*

$$\lim_{n\to\infty} -\frac{1}{n}\log P\left(\left|\frac{1}{n}\sum_{i=1}^{n}\log|h_i| - \mu\right| > \varepsilon\right) = A > 0, \quad (20)$$

then the probability of error $P_e(\Lambda)$ in Theorem 2 decays exponentially to zero.

This is the case, for instance, of non-degenerate iid (following from the Cramer-Chernoff bound). For more general processes satisfying this hypothesis see e.g. [14]. An explicit calculation for the Rayleigh fading process can be found in [8, Eq. (6)].

We close this section with a remark on the role of the ring of integers in the proof of Theorem 2. The function $g(x)$ (Equation (18)) used in our version of the Minkowski-Hlawka theorem is naturally bounded due to Lemma 2. Intuitively, the ring of integers protects the channel from deep fadings. For general lattices not constructed for number fields this need not be true. A way to circumvent this problem [6] is to assume regularity conditions on the fading process which essentially guarantees a sufficient fast decay of the probability of deep fadings. However, apart from questions of generality, this assumption degrades the probability of error to $O(1/n^2)$.

V. Power-Constrained Model

For the power-constrained model, we shape the constellation using the discrete Gaussian distribution. Given a coding lattice Λ, the transmitter choses a point $\mathbf{x} \in \Lambda$ according to the distribution D_{Λ,σ_s}. It was proven in [13, Sec. V] that, in the receiver side, given $\mathbf{H}$, the estimate $\hat{\mathbf{x}}$ that maximizes the a-posteriori probability is

$$\hat{\mathbf{x}} = \arg\min_{x\in\Lambda} \|\mathbf{F}\mathbf{y} - \mathbf{R}\mathbf{x}\|, \quad (21)$$

where $\mathbf{R}$ and $\mathbf{F}$ are diagonal with

$$R_{ii} = \sqrt{\rho h_i^2 + 1} \text{ and } F_{ii} = \frac{\rho h_i}{\sqrt{\rho h_i^2 + 1}},\ \rho \triangleq \frac{\sigma_s^2}{\sigma^2}.$$

In other words, MAP decoding is equivalent to lattice decoding with a scaling coefficient in each dimension. Note that this is a generalization of the MMSE estimation for the Gaussian channel, in which case Equation (21) reduces to [15, Eq. 11] by taking $h_i = 1$. Consider the channel equation after scaling the received vector by $\mathbf{F}$:

$$\bar{\mathbf{y}} = \mathbf{F}\mathbf{y} = \mathbf{R}\mathbf{x} + \mathbf{z}', \quad (22)$$

where $\mathbf{z}' = (\mathbf{F}\mathbf{H} - \mathbf{R})\mathbf{x} + \mathbf{F}\mathbf{z}$ is the equivalent noise. It was also proven in [13, Sec. V] that $\mathbf{z}'$, given $(h_1, \ldots, h_n)$ is *sub-Gaussian* with parameter σ. Furthermore, the probability of error of lattice decoding for $\bar{\mathbf{y}}$ is

$$P_e(\Lambda) = E_{\mathbf{H}}\left[P(\mathbf{z}' \notin \mathcal{V}_{\mathbf{R}\Lambda})\right]. \quad (23)$$

Since MAP decoding performs at least as well as the decoder in the proof of Theorem 2, the probability $P_e(\Lambda) \to 0$ if

$$\gamma_\Lambda(\sigma^2) > e^{-E_h[\log(|r|)]} 2\pi e,$$

where $r = \rho h^2 + 1$.

Moreover, if Λ_n is a sequence of lattices with vanishing flatness factor (3) (the existence of such a sequence can be guaranteed by the Minkowski-Hlawka theorem, as in [16, Appendix III]) then the average power of the constellation $P \to \sigma_s^2$ and, from [16, Lemma 6], any rate

$$\begin{aligned} R &= \frac{1}{2}\log(2\pi e\sigma_s^2) - \frac{1}{n}\log(V(\Lambda)) - \varepsilon \\ &= \frac{1}{2}E_h[\log|r|] - \varepsilon = C - \varepsilon \end{aligned} \quad (24)$$

is achievable.

VI. Acknowledgments

The work of Antonio Campello was funded by FAPESP under grant 2014/20602-8. This work was supported in part by FP7 project PHYLAWS (EU FP7-ICT 317562).

References

[1] R. Zamir. *Lattice Coding for Signals and Networks*. Cambridge, 2014.
[2] Y. Yan, C. Ling, and X. Wu. Polar lattices: Where Arikan meets Forney. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 1292–1296, July 2013.
[3] N. di Pietro. *On Infinite and Finite Lattice Constellations for the Additive White Gaussian Noise Channel*. PhD thesis, Université de Bordeaux, 2014.
[4] F. Oggier and E. Viterbo. Algebraic Number Theory and Code Design for Rayleigh Fading Channels. *Commun. Inf. Theory*, 1(3):333–416, December 2004.
[5] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore. Good lattice constellations for both Rayleigh fading and Gaussian channels both Rayleigh fading and Gaussian channels. *IEEE Transactions on Information Theory*, 42(2):502–518, Mar 1996.
[6] S. Vituri. Dispersion analysis of infinite constellations in ergodic fading channels. *CoRR*, abs/1309.4638, 2013.
[7] A. Hindy and A. Nosratinia. Approaching the ergodic capacity with lattice coding. In *IEEE Global Communications Conference (GLOBECOM)*, pages 1492–1496, Dec 2014.
[8] R. Vehkalahti and L. Luzzi. Number field lattices achieve Gaussian and Rayleigh channel capacity within a constant gap. In *IEEE International Symposium on Information Theory (ISIT)*, pages 436–440, June 2015.
[9] H.-A. Loeliger. Averaging bounds for lattices and linear codes. *IEEE Transactions on Information Theory*, 43(6):1767–1773, Nov 1997.
[10] R. Vehkalahti, W. Kositwattanarerk, and F. Oggier. Constructions a of lattices from number fields and division algebras. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2326–2330, June 2014.
[11] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*, volume 1. Cambridge University Press, 2005.
[12] J. Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1999.
[13] A. Campello, C. Ling, and J.-C. Belfiore. Algebraic Lattice Codes Achieve the Capacity of the Compound Block-Fading Channel. *available on arXiv*, 2016.
[14] R. H. Schonmann. Exponential convergence under mixing. *Probability Theory and Related Fields*, 81(2):235–238, 1989.
[15] C. Ling and J.-C. Belfiore. Achieving AWGN Channel Capacity With Lattice Gaussian Coding. *IEEE Transactions on Information Theory*, 60(10):5918–5929, Oct 2014.
[16] C. Ling and D. Stehle L. Luzzi, J.-C. Belfiore. Semantically secure lattice codes for the gaussian wiretap channel. *Information Theory, IEEE Transactions on*, 60(10):6399–6416, Oct 2014.