Wiretap lattice codes from number fields with no small norm elements

Ong, Soon Sheng; Oggier, Frédérique

2014

Ong, S. S., & Oggier, F. Wiretap lattice codes from number fields with no small norm elements. Designs, Codes and Cryptography, in press.

<https://hdl.handle.net/10356/103869>

<https://doi.org/10.1007/s10623-014-9935-7>

© 2014 Springer Science+Business Media New York. This is the author created version of a work that has been peer reviewed and accepted for publication by Designs, Codes and Cryptography, Springer Science+Business Media New York. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1007/s10623-014-9935-7>].

Downloaded on 26 Apr 2023 20:52:18 SGT

Wiretap Lattice Codes from Number Fields with no Small Norm Elements

Soon Sheng Ong · Frédérique Oggier

Received: date / Accepted: date

Abstract We consider the problem of designing reliable and confidential lattice codes, known as wiretap lattice codes, for fast fading channels. We identify as code design criterion for finite lattice constellations a finite sum of inverse of algebraic norms, in fact the analogous for finite sums of the known criterion for infinite constellations, which motivates us to study totally real number fields with few elements of small norms, over which ideal lattices can be built to provide wiretap lattice codes. More precisely, we first narrow down our search to abelian number fields known to provide reliable lattice codes, among which we look for no small inert primes and large regulators.

Keywords Ideal Lattices · Wiretap Codes · Units

Mathematics Subject Classification (2000) 11T71 · 94B60

1 Introduction

Wiretap channels are broadcast channels that model the communication between two legitimate users, Alice and Bob, in the presence of an eavesdropper Eve. Wiretap codes aim at achieving both reliability and confidentiality via coding, by exploiting the noise that the eavesdropper experiences. Despite many works of information theoretic nature providing achievable rates and secrecy capacity results, explicit wiretap code constructions remain elusive for many classes of channels, such as additive white Gaussian noise (AWGN), fading and MIMO channels. Recently the secrecy gain and the flatness factor (see respectively [12] and [9]) have been proposed as code design criteria for AWGN wiretap channels, in order to

The research of S.S. Ong and F. Oggier for this work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07. Part of this work was presented at the International Workshop on Coding and Cryptography, Bergen, Norway, April 2013 [13].

Soon Sheng Ong · Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore
E-mail: SSONG1@e.ntu.edu.sg and frederique@ntu.edu.sg

maximize the confusion at the eavesdropper, and lattice codes satisfying the former criterion have been studied [8].

In this paper, we focus on fast fading channels instead. A code design criterion to increase the eavesdropper confusion has been computed in [2] for infinite constellations, which involves the minimization of a sum of inverse norms in number fields. This minimization has been addressed in [6, 7] via the use of Dedekind zeta functions, and similar sums have been looked at in the context of the Diversity Multiplexing Trade-Offs (DMT) [14].

Our main contribution is to prove in Section 2 an analogous code design criterion as that of [2], but for finite constellations, based on a clean upper bound on Eve's probability of correctly decoding, which strengthens the foundation of sums of inverse norms as a wiretap code design criterion. We then translate the problem of code design for fast fading channels into finding totally real number fields with suitable parameters: while a large regulator is known to be desirable [14], we suggest to consider number fields with no elements of small norms (Section 3). We then focus on number fields known to provide reliable ideal lattice codes, and search among them those with inert small primes and large regulator (Section 4).

2 Fast Fading Wiretap Channels

We consider communication over a wiretap channel, where a legitimate user Alice sends information to Bob, another legitimate user, in the presence of an eavesdropper Eve. We assume that transmission occurs over a fast Rayleigh fading channel, which models a channel where Alice, Bob and Eve all use a single antenna. We assume that perfect channel state information (CSI) is available at both receivers. Formally, Bob and Eve respectively receive the vectors $\mathbf{y}$ and $\mathbf{z}$ given by

$$\begin{aligned}\mathbf{y} &= \text{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \text{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e,\end{aligned}\tag{1}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the transmitted signal, $\mathbf{v}_b$ and $\mathbf{v}_e$ denote the Gaussian noise at Bob, respectively Eve's side, both with zero mean, and respective variance σ_b^2 and σ_e^2 , and

$$\text{diag}(\mathbf{h}_b) = \begin{pmatrix} |h_{b,1}| & & \\ & \ddots & \\ & & |h_{b,n}| \end{pmatrix}, \quad \text{diag}(\mathbf{h}_e) = \begin{pmatrix} |h_{e,1}| & & \\ & \ddots & \\ & & |h_{e,n}| \end{pmatrix}$$

are the channel matrices containing the fading coefficients where $h_{b,i}, h_{e,i}$ are complex Gaussian random variables with variance $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, so that $|h_{b,i}|, |h_{e,i}|$ are Rayleigh distributed, $i = 1, \dots, n$, with parameter $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$.

The goal of coding for a wiretap channel is two-fold: to ensure reliability for Bob, and confidentiality for Alice (or equivalently, confusion for Eve). The former is characterized by Bob's probability of error, while the latter is typically interpreted via the mutual information between Alice's message and what Eve receives. We will derive another characterization for Eve's confusion below.

2.1 A Code Design Criterion

In order to design wiretap codes for the fast Rayleigh fading channel, a design criterion has been proposed in [2] which relies on an approximation of Eve's probability $P_{c,e}$ of correctly decoding using a Taylor expansion, itself depending on the channel conditions. We will rederive this design criterion here by computing instead a clean upper bound on Eve's probability $P_{c,e}$, which furthermore holds for case of *finite* lattice constellations.

We assume that Alice performs lattice encoding, that is the message intended for Bob is a vector $\mathbf{x} \in \mathbb{R}^n$ which belongs to a lattice $\Lambda_b \subset \mathbb{R}^n$. To confuse Eve, Alice uses a standard technique for wiretap coding, that is coset coding: she chooses a sublattice Λ_e of Λ_b , and partitions Λ_b into a union of disjoint cosets of Λ_e . Every message sent by Alice is encoded into a coset of Λ_e , say $\mathbf{c} + \Lambda_e$ and for the actual transmission to happen, a point $\mathbf{c} + \mathbf{r}$ in this coset is chosen uniformly at random. The intuition behind this scheme is that coset encoding provides a labeling of the lattice points of Λ_b with a mixture of data bits (which label a coset) and random bits (taken inside Λ_e). What it should achieve is to permit Eve to decode the random bits, but not the data bits, which may be possible because of the difference of noises between the legitimate and the eavesdropper channel, and enhanced by a good design of Λ_e . The benefit of using lattice coset coding has been shown in [12] for the Gaussian channel. Furthermore, to get a wiretap code design criterion, an error probability analysis is provided, instead of the usual mutual information (though the connection between both is made explicit).

To treat the case of wiretap codes for fast fading channels, a similar error probability is performed [2] for infinite lattice constellations, relying on the fact that once the fading is fixed, we deal with a Gaussian channel, and can use the results of [12]. The fading case is then obtained by averaging over the fading coefficients.

Note that [12] gives a bound on Eve's probability of error assuming that the lattice constellation is infinite, while here, we will need a finite constellation. This means that we first need a finite constellation version of the bound of [12], which we compute next. Recall that a Gaussian wiretap channel is of the form (1) where both channel matrices are the identity matrix.

Proposition 1 *Suppose transmission over a Gaussian wiretap channel, where coset coding is performed using the nested lattices $\Lambda_e \subset \Lambda_b$, and a finite constellation is sent, determined by a bounded region $\mathcal{R}$ around the origin. Suppose that the Fourier transform of the characteristic function $\chi_{\mathcal{R}}$ is even. Then Eve's probability $P_{c,e}$ of correct decision is upper bounded by*

$$P_{c,e} \leq \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \text{vol}(\Lambda_b) \sum_{\mathbf{t} \in \Lambda_e \cap \mathcal{R}} e^{-\|\mathbf{t}\|^2/2\sigma_e^2},$$

where $\text{vol}(\Lambda_b)$ denotes the volume of Λ_b .

Proof Eve's probability $P_{c,e}$ of correct decision when doing coset decoding after transmission over a Gaussian channel is

$$P_{c,e} = \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \sum_{\mathbf{t} \in \Lambda_e \cap \mathcal{R}} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} d\mathbf{u} \quad (2)$$

where $\mathcal{V}(\Lambda_b)$ denotes the Voronoi region of Λ_b , and the sum over $\mathbf{t}$ takes into account the randomization introduced by coset encoding. Then

$$\begin{aligned} P_{c,e} &= \int_{\mathcal{V}(\Lambda_b)} \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \sum_{\mathbf{t} \in \Lambda_e \cap \mathcal{R}} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} d\mathbf{u} \\ &= \int_{\mathcal{V}(\Lambda_b)} \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \sum_{\mathbf{t} \in \Lambda_e} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} \chi_{\mathcal{R}}(\mathbf{t}) d\mathbf{u}, \end{aligned}$$

where $\chi_{\mathcal{R}}(\mathbf{t})$ is 1 if $\mathbf{t} \in \mathcal{R}$ and 0 otherwise.

Denote

$$f(\mathbf{t}) = e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} \chi_{\mathcal{R}}(\mathbf{t}).$$

The Poisson summation formula for lattices [3] holds and yields

$$\sum_{\mathbf{t} \in \Lambda_e} f(\mathbf{t}) = \text{vol}(\Lambda_e)^{-1} \sum_{\mathbf{t}^* \in \Lambda_e^*} \hat{f}(\mathbf{t}^*)$$

where Λ_e^* is the dual lattice of Λ_e . We next compute $\hat{f}(\mathbf{t}^*)$, which by definition is

$$\begin{aligned} \hat{f}(\mathbf{t}^*) &= \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{t}^*, \mathbf{v} \rangle} f(\mathbf{v}) d\mathbf{v} \\ &= \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{t}^*, \mathbf{v} \rangle} \underbrace{e^{-\frac{\|\mathbf{u}\|^2 - 2\langle \mathbf{u}, \mathbf{v} \rangle - \|\mathbf{v}\|^2}{2\sigma_e^2}}}_{f_1(\mathbf{v})} \underbrace{\chi_{\mathcal{R}}(\mathbf{v})}_{f_2(\mathbf{v})} d\mathbf{v} \\ &= \int_{\mathbb{R}^n} \hat{f}_1(\mathbf{t}^* - \mathbf{w}) \hat{f}_2(\mathbf{w}) d\mathbf{w}, \end{aligned}$$

using the convolution theorem, where

$$\begin{aligned} \hat{f}_1(\mathbf{w}) &= \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{w}, \mathbf{v} \rangle} e^{-\frac{\|\mathbf{u}\|^2 - 2\langle \mathbf{u}, \mathbf{v} \rangle - \|\mathbf{v}\|^2}{2\sigma_e^2}} d\mathbf{v} \\ &= \prod_{j=1}^n \int e^{-2\pi i w_j v_j} e^{-\frac{-u_j^2 - 2u_j v_j - v_j^2}{2\sigma_e^2}} dv_j \\ &= \prod_{j=1}^n e^{-\frac{u_j^2}{2\sigma_e^2}} \int e^{-2\left(\pi i w_j + \frac{u_j}{2\sigma_e^2}\right) v_j} e^{-\frac{v_j^2}{2\sigma_e^2}} dv_j \\ &= \prod_{j=1}^n \sqrt{2\pi\sigma_e^2} e^{-2\sigma_e^2 \pi^2 w_j^2} e^{2\pi i w_j u_j} \\ &= \sqrt{2\pi\sigma_e^2}^n e^{-2\sigma_e^2 \pi^2 \|\mathbf{w}\|^2} e^{2\pi i \langle \mathbf{w}, \mathbf{u} \rangle} \end{aligned}$$

using

$$\int_{\mathbb{R}} e^{-ax^2} e^{-2bx} dx = \sqrt{\pi/ae} e^{b^2/a}, \quad a > 0. \quad (3)$$

This shows that

$$\begin{aligned} \hat{f}(\mathbf{t}^*) &= \int_{\mathbb{R}^n} \hat{f}_1(\mathbf{t}^* - \mathbf{w}) \hat{f}_2(\mathbf{w}) d\mathbf{w} \\ &= \sqrt{2\pi\sigma_e^2}^n \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} e^{2\pi i \langle \mathbf{t}^* - \mathbf{w}, \mathbf{u} \rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w} \end{aligned}$$

and

$$\begin{aligned}
\sum_{\mathbf{t}^* \in \Lambda_e^*} \hat{f}(\mathbf{t}^*) &= \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^* \in \Lambda_e^*} e^{2\pi i \langle \mathbf{t}^*, \mathbf{u} \rangle} \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} e^{-2\pi i \langle \mathbf{w}, \mathbf{u} \rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w} \\
&= \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^* \in \Lambda_e^*} \cos(2\pi \langle \mathbf{t}^*, \mathbf{u} \rangle) \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} e^{-2\pi i \langle \mathbf{w}, \mathbf{u} \rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w} \\
&\leq \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^* \in \Lambda_e^*} \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} e^{-2\pi i \langle \mathbf{w}, \mathbf{u} \rangle} \hat{f}_2(\mathbf{w}) d\mathbf{w}
\end{aligned}$$

by noting that the sine term of the exponential averages out to zero when summing over all lattice points, and where the last inequality follows from the fact that the cosine term takes its maximum value (that is 1) when $\mathbf{u} \in \Lambda$.

Using a similar argument, write $e^{-2\pi i \langle \mathbf{w}, \mathbf{u} \rangle} = \cos(2\pi \langle \mathbf{w}, \mathbf{u} \rangle) - i \sin(2\pi \langle \mathbf{w}, \mathbf{u} \rangle)$ and note that for a given $\mathbf{u}$, the integral over $\mathbb{R}^n$ will make the sine term alternate, so that $-e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2}$ and $e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* + \mathbf{w}\|^2}$ both will appear as a factor of $i \sin(2\pi \langle \mathbf{w}, \mathbf{u} \rangle) \hat{f}_2(\mathbf{w})$ ($\hat{f}_2(\mathbf{w})$ is even by hypothesis), and the sum over all lattices averages out to zero, since the four terms $-e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2}$, $e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* + \mathbf{w}\|^2}$ and $-e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2}$, $e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* + \mathbf{w}\|^2}$ appear as a factor of $i \sin(2\pi \langle \mathbf{w}, \mathbf{u} \rangle) \hat{f}_2(\mathbf{w})$. Thus

$$\sum_{\mathbf{t} \in \Lambda_e} f(\mathbf{t}) \leq \text{vol}(\Lambda_e)^{-1} \sqrt{2\pi\sigma_e^2}^n \sum_{\mathbf{t}^* \in \Lambda_e^*} \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} \hat{f}_2(\mathbf{w}) d\mathbf{w}.$$

This yields a first upper bound on Eve's probability $P_{c,e}$ of making a correct decision:

$$\begin{aligned}
P_{c,e} &\leq \text{vol}(\Lambda_e)^{-1} \int_{\mathcal{V}(\Lambda_b)} \left(\sum_{\mathbf{t}^* \in \Lambda_e^*} \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} \hat{f}_2(\mathbf{w}) d\mathbf{w} \right) d\mathbf{u} \\
&= \frac{\text{vol}(\Lambda_b)}{\text{vol}(\Lambda_e)} \sum_{\mathbf{t}^* \in \Lambda_e^*} \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} \hat{f}_2(\mathbf{w}) d\mathbf{w}.
\end{aligned}$$

To obtain an expression which depends on Λ_e instead of Λ_e^* , we denote this time

$$f(\mathbf{t}^*) = \int_{\mathbb{R}^n} e^{-2\sigma_e^2 \pi^2 \|\mathbf{t}^* - \mathbf{w}\|^2} \hat{f}_2(\mathbf{w}) d\mathbf{w},$$

and the Poisson summation formula for lattices now gives

$$\sum_{\mathbf{t}^* \in \Lambda_e^*} f(\mathbf{t}^*) = \text{vol}(\Lambda_e) \sum_{\mathbf{t} \in \Lambda} \hat{f}(\mathbf{t})$$

where $\hat{f}(\mathbf{t}) = \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{t}, \mathbf{v} \rangle} f(\mathbf{v}) d\mathbf{v}$, and we recognize that $\hat{f}(\mathbf{t})$ is actually the Fourier transform of the convolution of $e^{-2\sigma_e^2 \pi^2 \|\mathbf{v}\|^2}$ and $\hat{f}_2(\mathbf{v})$. We then obtain

the product of Fourier transforms, that is

$$\begin{aligned}
\hat{f}(\mathbf{t}) &= \left(\int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{t}, \mathbf{v} \rangle} e^{-2\pi^2 \sigma_e^2 \|\mathbf{v}\|^2} d\mathbf{v} \right) f_2(\mathbf{t}) \\
&= \left(\prod_{j=1}^n \int_{\mathbb{R}} e^{-2\pi i t_j v_j} e^{-2\pi^2 \sigma_e^2 v_j^2} dv_j \right) f_2(\mathbf{t}) \\
&= \left(\frac{1}{\sqrt{2\pi\sigma_e^2}} \right)^n \prod_{j=1}^n e^{\frac{-t_j^2}{2\sigma_e^2}} \chi_{\mathcal{R}}(\mathbf{t}) \\
&= \left(\frac{1}{\sqrt{2\pi\sigma_e^2}} \right)^n e^{-\frac{\|\mathbf{t}\|^2}{2\sigma_e^2}} \chi_{\mathcal{R}}(\mathbf{t})
\end{aligned}$$

using again (3).

Finally the probability of making a correct decision for Eve is summarized by

$$P_{c,e} \leq \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \text{vol}(\Lambda_b) \sum_{\mathbf{t} \in \Lambda_e \cap \mathcal{R}} e^{-\|\mathbf{t}\|^2 / 2\sigma_e^2}. \quad (4)$$

Remark 1 One may take the region $\mathcal{R}$ to be a cube centered around the origin. This will satisfy the hypothesis of the proposition. In the case the shaping region does not satisfy the hypothesis it can always be inserted into a cube of the right size, which will serve as an upper bound.

Corollary 1 *Suppose transmission over a fast fading wiretap channel as described in 1, where coset coding is performed using the lattices $\Lambda_e \subset \Lambda_b$, under the same hypothesis as in the above proposition. Then Eve's average probability $\bar{P}_{c,e}$ of correct decision is upper bounded by*

$$\bar{P}_{c,e} \leq \left(\frac{\sigma_{h,e}^2}{\sigma_e^2} \right)^{n/2} \text{vol}(\Lambda_b) \sum_{\mathbf{x} \in \Lambda_e \cap \mathcal{R}} \prod_{i=1}^n \frac{1}{\left(1 + |x_i|^2 (\sigma_{h,e}^2 / \sigma_e^2) \right)^{3/2}}.$$

Proof The proof technique is the same as that of [2]. Once the fading coefficients are fixed, the channel (1) becomes a Gaussian wiretap channel, where the lattice point sent now belongs to a new lattice which includes the fading matrix: if $\mathbf{x}$ is a lattice point of the form $\mathbf{x} = M\mathbf{u}$, $\mathbf{u} \in \mathbb{Z}^n$, where M is the generator matrix of the lattice in use, then $\text{diag}(\mathbf{h}_b)M\mathbf{u}$ still belongs to a lattice, with generator matrix $\text{diag}(\mathbf{h}_b)M$. The upper bound of the proposition is then used, and the average probability of error is computed over different fading realizations (using that the coefficients are Rayleigh distributed).

Remark 2 Note that the upper bound in the above corollary is very similar to that obtained for Bob's probability of error for fast fading channels classically [11], except for the sum. Indeed, Bob, who is in that case, is not affected by the randomization introduced by Λ_e , since Alice transmits based on Bob's channel. The usual design for fast fading channels is then simplified to give that

$$\frac{1}{\prod_{x_i \neq 0} |x_i|} \quad (5)$$

should be minimized, and in particular the n components of every lattice point should be non-zero, property referred to as *full diversity*.

The same simplification, which may not give the best bound but a first understanding of the situation, yields as wiretap code design criterion to minimize

$$\sum_{\mathbf{x} \in \Lambda_e \cap \mathcal{R}, \mathbf{x} \neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3} \quad (6)$$

where $\mathbf{x} = (x_1, \dots, x_n)$. A first observation is that, as for Bob's case (5), it is desirable to have as many non-zero coefficients as possible among the x_i . Ideally, we would like all the non-zero vectors $\mathbf{x} \in \Lambda_e$ to have only non-zero coefficients. Given a vector $\mathbf{x}$ of length n , its *diversity* is the number of its non-zero coefficients. Given an n -dimensional lattice, its diversity is the minimum diversity over every non-zero lattice vector, and we are again looking for full diversity (where the diversity is the length n of the vector). The property of diversity is well understood in the context of *ideal lattices*.

2.2 Ideal Lattices

Let K be a number field, that is an extension of $\mathbb{Q}$, of degree n , and let $\sigma_1, \dots, \sigma_{r_1}$ be the r_1 real embeddings of K , and $\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}$ be the complex embeddings of K , which come in r_2 pairs of conjugates. We have that $n = r_1 + 2r_2$. If $r_2 = 0$, we say that K is a *totally real* number field. For $x \in K$, recall that the *trace* of x over $\mathbb{Q}$ is defined as $\text{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$, while the *norm* of x is defined as $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^n \sigma_i(x)$.

From now on, we assume that K is a totally real number field of degree n ($n = r_1$), with ring of integers $\mathcal{O}_K$, and real embeddings $\sigma_1, \dots, \sigma_n$.

Definition 1 An *ideal lattice* is an integral lattice formed by an $\mathcal{O}_K$ -ideal $\mathcal{I}$ (which may be fractional) and a positive definite symmetric bilinear form q_α :

$$q_\alpha : \mathcal{I} \times \mathcal{I} \rightarrow \mathbb{Z}, \quad q_\alpha(x, y) = \text{Tr}_{K/\mathbb{Q}}(\alpha xy), \quad \forall x, y \in \mathcal{I}$$

where $\alpha \in \mathcal{O}_K$ is totally positive (i.e., $\sigma_i(\alpha) > 0$ for all i).

The element α has a “twisting” effect which is useful to obtain different types of lattices over the same ring of integers. In fact, α could be taken outside $\mathcal{O}_K$ under different conditions, but the case where $\alpha \in \mathcal{O}_K$ is enough for our purpose.

If $\{\omega_1, \dots, \omega_n\}$ is a $\mathbb{Z}$ -basis of $\mathcal{I}$, the generator matrix M of the corresponding ideal lattice $\Lambda_{\mathcal{I}} = \{\mathbf{x} = M\mathbf{u} | \mathbf{u} \in \mathbb{Z}^n\}$ is given by

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \dots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix}^T \quad (7)$$

where $\alpha_j = \sigma_j(\alpha)$, for all j . One easily verifies that the Gram matrix $M^T M$ is given by $\{\text{Tr}(\alpha \omega_i \omega_j)\}_{i,j=1}^n$. The volume $\text{vol}(\Lambda_{\mathcal{I}})$ of this lattice is [1]

$$\text{vol}(\Lambda_{\mathcal{I}}) = \det(\{\text{Tr}(\alpha \omega_i \omega_j)\}_{i,j=1}^n)^{1/2} = (N(\alpha)N(\mathcal{I})^2 d_K)^{1/2} \quad (8)$$

where d_K is the discriminant of K . Different authors use different conventions for the volume, it could be either $\det(M^T M)$ or $\det(M^T M)^{1/2}$.

Ideal lattices are defined over a number field, irrespectively of its *signature* (r_1, r_2) . However, when $r_2 = 0$ as assumed above, the diversity of the resulting lattice is maximal, that is $n = r_1$. Indeed, if $\mathbf{x}$ is a non-zero vector in this ideal lattice, then

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(\sum_{i=1}^n u_i\omega_i), \dots, \sqrt{\alpha_n}\sigma_n(\sum_{i=1}^n u_i\omega_i)),$$

but if $x_j = \sqrt{\alpha_j}\sigma_j(\sum_{i=1}^n u_i\omega_i) = 0$ for some j , then $\sum_{i=1}^n u_i\omega_i = 0$ and every x_i must be zero, a contradiction.

When choosing Λ_e to be an ideal lattice from a totally real number field K of degree n , (6) becomes

$$\begin{aligned} \sum_{\mathbf{x} \in \Lambda_e \cap \mathcal{R}, \mathbf{x} \neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3} &= \sum_{x \in \mathcal{I} \cap \mathcal{R}', x \neq 0} \prod_{i=1}^n \frac{1}{(\sqrt{\alpha_i}|\sigma_i(x)|)^3} \\ &= \sum_{x \in \mathcal{I} \cap \mathcal{R}', x \neq 0} \frac{1}{(\sqrt{N_{K/\mathbb{Q}}(\alpha)}|N_{K/\mathbb{Q}}(x)|)^3} \end{aligned} \quad (9)$$

since $\mathbf{x} = (x_1, \dots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \dots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^n u_i\omega_i \in \mathcal{I}$, and $\mathcal{R}'$ is some subset of $\mathcal{I}$ corresponding to $\mathcal{R}$. In this paper, we will mostly consider the case where K is a Galois extension, and $\mathcal{I}$ is a principal, to start with (in whole generality, a Galois extension is not needed to build an ideal lattice, and the ideal does not have to be principal). In that case, $x \in \mathcal{I} = (\beta)\mathcal{O}_K$, $N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(x')$ for some $x' \in \mathcal{O}_K$, and we see from (9) that the sum which becomes of interest is

$$\sum_{x \in \mathcal{O}_K \cap \mathcal{B}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}. \quad (10)$$

We write $\mathcal{B}$ to emphasize that we are interested in finite sums, ideally $\mathcal{B}$ should be computed as a function of $\mathcal{R}$, though that may not always be easy to do.

It is worth noting that since Λ_e is a sublattice of Λ_b , both lattices will be obtained as ideal lattices over $\mathcal{O}_K$. This is consistent with the design of Λ_b , since this lattice will also benefit of the full diversity property coming from choosing K totally real, and full diversity is indeed a design criterion for reliability over fast Rayleigh fading channels (see Remark 2).

2.3 A Wiretap Code Design Criterion

To summarize the computations done so far, the wiretap code design criterion for two nested ideal lattice codes $\Lambda_e \subset \Lambda_b$ becomes, in terms of the underlying number field K of degree n :

1. Minimize $\min_{x \in \mathcal{O}_K, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|}$, which determines the coding gain of the ideal lattice code, this is assuming that full diversity is achieved, which is guaranteed by choosing K to be totally real. The coding gain ranks totally real number fields of the same degree, and thus is the second code design for reliability after full diversity.

2. Minimize $\sum_{x \in \mathcal{O}_K \cap \mathcal{B}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$, which characterizes the confusion at the eavesdropper.

While the first optimization is well understood (see e.g. [11]), the second one is being currently investigated, while the joint design is mainly open.

Let us make a first obvious remark regarding (10). If $\mathcal{B}$ were an infinite region, this sum will not be finite in most of the cases. Indeed, for it to be finite, we need $\mathcal{O}_K$ to contain finitely many elements of norm 1, that is finitely many *units*. It is known (this is Dirichlet's unit Theorem) that the group of units of K is finitely generated and has rank $r_1 + r_2 - 1$, as a result, the rank will always be strictly positive, except for quadratic imaginary fields (for which $r_1 = 0$ and $r_2 = 1$).

Next, the dominant terms in the sum (10) are integers with small norms. The contribution of the terms of norm 1 depends on the density of units, while that of elements of norm at least 2 depends on the ramification in K , the class number of K (which we will not study since the examples we will consider all have a class number of 1), and also the density of units (since if x has a given norm, then ux where u is a unit will have the same norm). The important role that units play is well understood asymptotically [14]. The role of elements of small norms in our case is not straightforward. We will thus be interested next in deriving a criterion to obtain number fields with a specific ramification, to ensure that there is no element with a small norm. This guarantees that small norm elements will not contribute to the sum (10). This is done in Section (3). We will consider the density of units in Section (4).

Remark 3 Once the role of units and small norms (if any) will be well understood, the final optimization will need two more ingredients, to be able to compare coding strategies: one is the design of the shaping region that determines the finite lattice constellation, the other one is the normalization of lattices. It is important to keep in mind that we are comparing two coding strategies via (10), and for such a comparison to make sense, lattices Λ_e of same volume should be compared. In particular, choosing an ideal of big norm is not a valid strategy, since it essentially inflates the volume of the lattice considered.

3 Number Fields and Elements of Small Norms

We are interested in making sure that elements of small norms are not contributing to the sum (10). We will thus next look for conditions on the ramification, namely make sure that small primes stay inert. Note that elements of small norms may alternatively be considered as a second design criterion, namely, one could optimize (10) and then, if needed, use the results of this section to distinguish number fields with a similar unit density.

3.1 Norms and Ramification

Let p be a prime, then p belongs to the ideal $p\mathcal{O}_K$, and by considering the prime factorization of $p\mathcal{O}_K$, we have

$$N(p\mathcal{O}_K) = N\left(\prod_{i=1}^g \mathfrak{p}_i^{e_i}\right) = \prod_{i=1}^g N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals. If K is Galois, then $p\mathcal{O}_K = \prod_{i=1}^g \mathfrak{p}_i^e$, that is $e_i = e$ for all i .

In particular, if p is totally ramified ($g = 1$ and $e_1 = n$) or if p totally splits ($g = n$ and all the ramification indices are 1), then

$$N(\mathfrak{p})^n = p^n, \text{ or } \prod_{i=1}^n N(\mathfrak{p}_i) = p^n$$

shows the existence of an ideal above p of norm p . If this ideal is principal, then the generators will have norm p . This argument shows how to find elements of norm p , but also that having $e = g = 1$ will force the smallest norm involving only the prime p to be at least p^n . Indeed, suppose that there exists an element $x \in \mathcal{O}_K$ whose norm is p^j for some positive j . Then $N((x)\mathcal{O}_K) = |N_{K/\mathbb{Q}}(x)| = p^j$ and by definition $|\mathcal{O}_K/(x)\mathcal{O}_K| = p^j$, which shows that $p^j \subset (x)\mathcal{O}_K$, thus $(p^j)\mathcal{O}_K \subset (x)\mathcal{O}_K$ and $(x)\mathcal{O}_K | (p^j)\mathcal{O}_K$. Since $(p)\mathcal{O}_K$ is prime ($e = g = 1$), it must be that $(x)\mathcal{O}_K = (p)^{j'}\mathcal{O}_K$ for some $j' \leq j$, and $N((x)\mathcal{O}_K) = N((p)\mathcal{O}_K)^{j'} = p^{nj'}$, showing that $j \geq n$.

3.2 Maximal Real Subfields of Cyclotomic Fields

Let ζ_p denote a primitive p th root of unity, and consider the cyclotomic field $\mathbb{Q}(\zeta_p)$. It has degree $p - 1$ over $\mathbb{Q}$, and its maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ has degree $(p - 1)/2$ over $\mathbb{Q}$. They have respective rings of integers $\mathbb{Z}[\zeta_p]$ and $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. The ring of integers $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ is known to provide efficient ideal lattices codes for Rayleigh fading channels [11]. The ramification in $\mathbb{Q}(\zeta_p)$ is well understood.

Theorem 1 [10] *Let q be a rational prime different from p , then q is unramified in $\mathbb{Q}(\zeta_p)$ and in fact*

$$(q)\mathbb{Z}[\zeta_p] = \mathfrak{q}_1 \dots \mathfrak{q}_g$$

with mutually distinct prime ideals $\mathfrak{q}_i$ and each of inertial degree $f = f(\mathfrak{q}_i/q)$ equal to the order of q in $(\mathbb{Z}/p)^\times$, i.e., f is the least natural number such that

$$q^f \equiv 1 \pmod{p}.$$

Since we will be looking at subfields of $\mathbb{Q}(\zeta_p)$, it is useful to remember that the ramification and the residual index satisfy transitivity, namely

$$e(\mathfrak{q}_L/q) = e(\mathfrak{q}_L/\mathfrak{q}_K)e(\mathfrak{q}_K/q), \quad f(\mathfrak{q}_L/q) = f(\mathfrak{q}_L/\mathfrak{q}_K)f(\mathfrak{q}_K/q), \quad (11)$$

for the tower $L/K/\mathbb{Q}$ and $\mathfrak{q}_L$ a prime above $\mathfrak{q}_K$, and $\mathfrak{q}_K$ a prime above q .

Consider the special case when $p = 2p' + 1$, with p' a prime. It is then easy to make sure that small primes stay inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Lemma 1 Suppose that $p = 2p' + 1$, where both p and p' are prime (such a prime p' is called a Sophie Germain prime). Then the primes smaller than p are inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Proof Let q be a prime smaller than p . By forcing $p = 2p' + 1$ with p' prime, the degree of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is now p' over $\mathbb{Q}$. Since

$$p' = e(\mathfrak{q}_i/q)f(\mathfrak{q}_i/q)g(\mathfrak{q}_i/q)$$

for every prime $\mathfrak{q}_i$ above q and $e(\mathfrak{q}_i/q) = 1$ when q is distinct from p (if $e(\mathfrak{q}_i/q) > 1$, then by transitivity (11) q should ramify in $\mathbb{Q}(\zeta_p)$), we deduce that either (1) $f(\mathfrak{q}_i/q) = 1$ and $g(\mathfrak{q}_i/q) = p'$, or (2) $f(\mathfrak{q}_i/q) = p'$ and $g(\mathfrak{q}_i/q) = 1$. But $f(\mathfrak{q}_i/q) = 1$ implies that either $q \equiv 1 \pmod{p}$, or $q^2 \equiv 1 \pmod{p}$.

The former case cannot happen if q is smaller than p .

The latter case is also impossible. Here are two reasons why this is the case. Firstly: $q^2 \equiv 1 \pmod{p}$ means that q is an element of order 2. But in the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, generated by some element a , the elements of order 2 are of the form a^k with $(p-1)/\gcd(p-1, k) = 2$, that is $2p'/\gcd(2p', k) = 2$, implying that k must be an odd multiple of p' , that is $k = p'$. Now this element of order 2 has to be $a^{p'} = p - 1$, since $(p-1)^2 \equiv 1 \pmod{p}$. Alternatively: $q^2 \equiv 1 \pmod{p}$ is equivalent to $(q-1)(q+1) \equiv 0 \pmod{p}$, that is p divides $(q-1)$ or $(q+1)$. But $q < p$ so p cannot divide $(q-1)$, and p cannot divide $q+1$ either, since $p-1$ is even.

This shows that $f(\mathfrak{q}_i/q) = p'$ and q is inert.

Example 1 Consider $\mathbb{Q}(\zeta_{23})$, with $23 = 2 \cdot 11 + 1$. The primes 2, 3, 5, 7, 11, 13, 17, 19 are all inert in $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$.

We could extend this technique to consider a totally real subfield K of $\mathbb{Q}(\zeta_p)$ of degree $[K : \mathbb{Q}] = p'$, when $p = mp' + 1$. Indeed, the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, that is, it is a cyclic group of order $p-1 = mp'$. Let us denote by σ its generator. Then $\sigma^{p'}$ generates a subgroup of order m , to which corresponds a subfield $K = \mathbb{Q}(\zeta_p)^{\langle \sigma^{p'} \rangle}$ which is fixed by $\langle \sigma^{p'} \rangle$, which is of degree p' over $\mathbb{Q}$. Since p' is prime, the same argument as in the proof of Lemma 1 shows that if q is a prime different from p , then q cannot ramify. Either it is inert, or it splits totally.

Example 2 Consider $\mathbb{Q}(\zeta_{67})$, with $67 = 6 \cdot 11 + 1$. Let σ be the generator of the Galois group of $\mathbb{Q}(\zeta_{67})/\mathbb{Q}$. The subgroup $\langle \sigma^{11} \rangle$ has order 6, with corresponding fixed field K , which is totally real and of degree 11 over $\mathbb{Q}$. Its minimal polynomial is $X^{11} - X^{10} - 30X^9 + 63X^8 + 220X^7 - 698X^6 - 101X^5 + 1960X^4 - 1758X^3 + 35X^2 + 243X + 29$. Since

$$11 = f(\mathfrak{q}_i/q)g(\mathfrak{q}_i/q)$$

we have that $f(\mathfrak{q}_i/q)$ is either 1 or 11. Let us assume that this is 1. Using the transitivity formula (11)

$$f(\mathfrak{q}_L/q) = f(\mathfrak{q}_L/\mathfrak{q}_i)$$

thus $f(\mathfrak{q}_L/q)$ is either 1, 2, 3, or 6, with $L = \mathbb{Q}(\zeta_{67})$. A direct computation using Theorem 1 shows that 2, 3, 5, 7, 11, 13, 17, 19 and 23 are inert. On the other hand, $29^3 \equiv 1 \pmod{67}$.

Fig. 1 A cyclotomic field $\mathbb{Q}(\zeta_p)$ with p prime and its subfield of degree $(p-1)/f$ for f a divisor of $p-1$.

$$\begin{array}{ccc}
 L = \mathbb{Q}(\zeta_p) & \supset & \mathfrak{q}_{K,1}\mathcal{O}_L = \mathfrak{q}_{L,1} \cdots \mathfrak{q}_{L,s} \\
 \downarrow f \mid G_f & & \\
 K = \mathbb{Q}(\zeta_p)^{\langle \sigma^f \rangle} & \supset & \mathfrak{q}\mathcal{O}_K = \mathfrak{q}_{K,1} \cdots \mathfrak{q}_{K,r} \\
 \downarrow e=(p-1)/f \mid G/G_f & & \\
 \mathbb{Q} & &
 \end{array}$$

3.3 Other Totally Real Subfields of Cyclotomic Fields

We next consider more generally totally real subfields of $\mathbb{Q}(\zeta_p)$, with p a prime. As recalled above, the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, that is, it is a cyclic group of order $p-1$. Let us denote by σ its generator. If $f \mid p-1$, set $e = (p-1)/f$. Then σ^f generates a subgroup of order f , that we denote by G_f , to which corresponds a subfield $K = \mathbb{Q}(\zeta_p)^{\langle \sigma^f \rangle}$ which is fixed by $G_f = \langle \sigma^{p'} \rangle$, which is of degree e over $\mathbb{Q}$ (see Figure 1). The Galois group of $K/\mathbb{Q}$ is the quotient group G/G_f . Let $q \in \mathbb{Z}$ be a prime, $q \neq p$, and let $\mathfrak{q}_K \in \mathcal{O}_K$ be a prime lying over q , and $\mathfrak{q}_L \in \mathcal{O}_L$ be a prime lying over $\mathfrak{q}_K$. The decomposition groups $D_{\mathfrak{q}_K}$ of $\mathfrak{q}_K$ and $D_{\mathfrak{q}_L}$ of $\mathfrak{q}_L$ are respectively, by definition, the groups

$$D_{\mathfrak{q}_L} = \{\sigma \in G, \sigma(\mathfrak{q}_L) = \mathfrak{q}_L\}, \quad D_{\mathfrak{q}_K} = \{\tau \in G/G_f, \tau(\mathfrak{q}_K) = \mathfrak{q}_K\}.$$

It is known that

$$g(\mathfrak{q}_K/q) = [G/G_f : D_{\mathfrak{q}_K}] = r, \quad g(\mathfrak{q}_L/q) = [G : D_{\mathfrak{q}_L}] = s$$

giving us a way to determine whether $r = 1$ (that is q is inert in K) using decomposition groups. Now let $\mathbb{Q}(\zeta_p)^{D_{\mathfrak{q}_L}} = L^{D_{\mathfrak{q}_L}}$ be the subfield of L fixed by $D_{\mathfrak{q}_L}$. Since q cannot ramify in L , $e(\mathfrak{q}_L/q) = 1$ and

$$p-1 = f(\mathfrak{q}_L/q)g(\mathfrak{q}_L/q) = [L : L^{D_{\mathfrak{q}_L}}][L^{D_{\mathfrak{q}_L}} : \mathbb{Q}] = |D_{\mathfrak{q}_L}| |G/D_{\mathfrak{q}_L}|$$

showing that $|D_{\mathfrak{q}_L}| = f(\mathfrak{q}_L/q)$, that is, $D_{\mathfrak{q}_L}$ is a subgroup of the cyclic group $G = \langle \sigma \rangle$ of order $f(\mathfrak{q}_L/q)$, which is the order of $q \pmod{p}$ (by the previous theorem). We are then left to compute $g(\mathfrak{q}_K/q) = [G/G_f : D_{\mathfrak{q}_K}] = r$, that is the index of the subgroup generated by the image of q in G/G_f , which can be computed to be $(p-1)/\text{lcm}(f, f(\mathfrak{q}_L/q))$. In summary:

Proposition 2 *Let K be a subfield of $\mathbb{Q}(\zeta_p)$ for p a prime, and let $q \neq p$ be a prime. Suppose that $[K : \mathbb{Q}] = (p-1)/f$, for f some divisor of $p-1$. If the least common multiple of f and of the order of $q \pmod{p}$ is $p-1$, then q is inert in K .*

Since we are interested in comparing different number fields, we will start by looking at fields of degree 5. For that, we will apply this proposition on subfields of the cyclotomic fields $\mathbb{Q}(\zeta_p)$ with $p = 2m+1$ and $5 \mid m$. Indeed, in this case, its maximal real subfield has degree m , and we will find a suitable subfield. This gives us $p \in \{11, 31, 41, 61, 71\}$.

Example 3 The prime 3 splits in $\mathbb{Q}(\zeta_{41})$ since $f = 8$ and the order of 3 (mod 41) is 8, thus $g(\mathfrak{q}_K/3) = 5$.

Example 4 The prime 2 is inert in $\mathbb{Q}(\zeta_{31})$ since $f = 6$ and the order of 2 (mod 31) is 5, thus $(p-1)/\text{lcm}(6, 5) = 1$. Similary, 3 is inert, since the order of 3 mod 31 is 30. On the other hand, 5 splits, since the order of 5 (mod 31) is 3 and $g(\mathfrak{q}_K/5) = 30/\text{lcm}(3, 6) = 5$.

Similar computations show that 11 and 23 are the smallest primes which are not inert in $\mathbb{Q}(\zeta_{61})$ and $\mathbb{Q}(\zeta_{71})$ respectively.

To conclude this section on elements of small norms, we provide an example that illustrates the role that elements of small norm may play in understanding (10). To evaluate (10), a bounding region is needed. We use a simplistic region to simplify the computations. It will however be needed to compute a proper shaping region for a definite conclusion.

Example 5 Consider the number field $K_1 = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, where ζ_{16} is a primitive 16th root of unity. It is of degree $\varphi(16)/2 = 4$ over $\mathbb{Q}$, has ring of integers $\mathcal{O}_{K_1} = \mathbb{Z}[\zeta_{16} + \zeta_{16}^{-1}]$ and discriminant $d_{K_1} = 2048$ and regulator $R_{K_1} = 2.44$. It contains elements of norm 2 (in particular $(1 - \zeta_{16})(1 - \zeta_{16}^{-1})$ has norm 2). We take as an integral basis $\nu_i = (\zeta_{16} + \zeta_{16}^{-1})^i$, $i = 0, 1, 2, 3$ and $\mathcal{B}(b) = \{\sum_{i=0}^3 a_i \nu_i, a_i \in [-b, \dots, b]\}$. Consider next the number field K_2 with minimal polynomial $X^4 - X^3 - 5X^2 + 2X + 4$ and discriminant $d_{K_2} = 2225$ and regulator $R_{K_2} = 2.06$. We take as integral basis (computed numerically using a specialized software, such as SAGE and KASH) $\mu_i = \theta^i$, $i = 0, 1, 2$ and $\mu_3 = (\theta + \theta^2 + \theta^3)/2$, where θ is a root of the minimal polynomial, with $\mathcal{B}(b) = \{\sum_{i=0}^3 a_i \mu_i, a_i \in [-b, \dots, b]\}$. Elements of small norms as well as (10) for different choices of $\mathcal{B}(b)$ are computed numerically and shown in Table 1. We observe that K_2 gives smaller sums for the three choices of b , despite having a larger number of units every time ($[1, x]$ refers to x elements having a norm whose absolute value is 1). The two regulators are very close to each other, $R_{K_2} = 2.06 < R_{K_1} = 2.44$ which is consistent with the fact that K_2 has a larger density of units, thus in this case, the elements of norm 2 do distinguish these two number fields with very close regulators. This illustrates the weight of the elements of norm 2 in the sum, and the fact that they cannot be neglected. Furthermore, elements of norm up to 4 are enough here to describe the behavior of the sums. For example for K_1 and $b = 4$ (but this is true for every case)

$$120 + \frac{92}{2^3} + \frac{84}{4^3} = 120 + 11.5 + 1.3125 = 132.8125 \simeq 133.$$

These two fields were chosen for a fair comparison, since they are both totally real, have the same degree, and discriminants close to each other. To make things even more complicated, the above computations are sensible to a choice of integral basis. For example, for K_2 , another integral basis is $\{1, (\theta + \theta^2 + \theta^3)/2, \theta^2, \theta^3\}$, which yields as small norms $[1, 96], [4, 120]$ and sum 97.90 for $b = 4$, $[1, 226], [4, 290]$ and sum 230.61 for $b = 8$ and $[1, 414], [4, 566]$ with sum 422.99 for $b = 15$.

4 Units and Regulators

Let K be a number field of degree d and signature (r_1, r_2) . Set $r = r_1 + r_2 - 1$. The density of units in K is related to its regulator R .

Table 1 The sum (10) is computed for K_1 (in the 2nd column) and K_2 (in the 3rd column) for different values of b (in the 1st column). We observe that K_2 gives smaller sums, despite a higher number of units (in the 4th and 5th columns, $[x, y]$ refers to the number of elements y with norm in absolute value equal to x).

b	K_1	K_2	small norms in K_1	small norms in K_2
$b = 4$	133.00	130.43	$[1, 120], [2, 92], [4, 84]$	$[1, 128], [4, 152]$
$b = 8$	281.71	269.68	$[1, 252], [2, 212], [4, 178]$	$[1, 264], [4, 354]$
$b = 15$	491.07	479.09	$[1, 438], [2, 378], [4, 320]$	$[1, 468], [4, 690]$

Table 2 Some totally real number fields K with their small primes and regulator. The first column describes K as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, the second column is the regulator R , the third column is the minimal polynomial of K , and the fourth column gives the first small prime which is not inert.

$K \subset \mathbb{Q}(\zeta_p)$	R	$p(X)$	primes
$\mathbb{Q}(\zeta_{11})$	1.63	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	11 ramifies
$\mathbb{Q}(\zeta_{31})$	30.37	$X^5 - 9X^4 + 20X^3 - 5X^2 - 11X - 1$	5 splits
$\mathbb{Q}(\zeta_{61})$	93.768	$X^5 + X^4 - 24X^3 - 17X^2 + 41X - 13$	11 splits
$\mathbb{Q}(\zeta_{71})$	70.611	$X^5 + X^4 - 28X^3 + 37X^2 + 25X + 1$	23 splits
$\mathbb{Q}(\zeta_{23})$	1014.31	$X^{11} + X^{10} - 10X^9 - 9X^8 + 36X^7 + 28X^6 - 56X^5 - 35X^4 + 35X^3 + 15X^2 - 6X - 1$	23 ramifies
$\mathbb{Q}(\zeta_{67})$	330512.24	$X^{11} - X^{10} - 30X^9 + 63X^8 + 220X^7 - 698X^6 - 101X^5 + 1960X^4 - 1758X^3 + 35X^2 + 243X + 29$	29 splits

Definition 2 Given a basis $e_1, \dots, e_r$ for the group of units modulo the group of roots of unity. The *regulator* of K is

$$R = |\det(\log |\sigma_i(e_j)|)_{1 \leq i, j \leq r}|,$$

where $|\sigma_i(e_j)|$ denotes the absolute value for the real embeddings, and the square of the complex absolute value for the complex ones.

Let w be the number of roots of unity in K . The best known bound on the number of units is given in [4].

Theorem 2 The number of units $U(q)$ such that $\max_{1 \leq i \leq d} |\sigma_i(u)| < q$ in K is given by

$$U(q) = \frac{w(r+1)^r}{Rr!} (\log q)^r + O((\log q)^{r-1-(cR^{2/r})^{-1}})$$

as $q \rightarrow \infty$ and $c = 6 \cdot 2 \cdot 10^{12} d^{10} (1 + 2 \log d)$.

We might use this result on $U(q)$ to evaluate the amount of units in the region $\mathcal{B}$ of interest, that is of elements of norm 1 in (10), since one can always take the maximum of $\max_{1 \leq i \leq d} |\sigma_i(u)|$ over every unit in $\mathcal{B}$ to define q . Since we focus on totally real number fields, $w = 2$ (the only roots of unity are ± 1), $r_2 = 0$ and $r_1 = d$, so that $r = d - 1$. Thus the regulator is the only factor that distinguishes two totally real numbers of same degree.

Unfortunately, results on regulators of number fields are not easily found. To have a sense of the range to which regulators belong, we compute numerically regulators corresponding to totally real number fields discussed in the previous section, including maximal totally real subfields of cyclotomic fields, known to be

Table 3 Some totally real number fields K with their small primes, discriminant d_K , regulator and class number h_K . The first column describes K as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, the second column is the regulator R , the third column is discriminant d_K of K , and the fourth column gives the first small prime which is not inert.

$K \subset \mathbb{Q}(\zeta_p)$	R	d_K	h_K	primes	(10) for $\mathcal{B}(6)$
$\mathbb{Q}(\zeta_{11})$	1.63	11^4	1	11 ramifies	1352.65
$\mathbb{Q}(\zeta_{31})$	30.36	31^4	1	5 splits	90.22
$\mathbb{Q}(\zeta_{61})$	93.768	61^4	1	11 splits	44.12
$\mathbb{Q}(\zeta_{71})$	70.611	71^4	1	23 splits	60.01
$\mathbb{Q}(\zeta_{23})$	1014.31	23^{10}	1	23 ramifies	
$\mathbb{Q}(\zeta_{67})$	330512.24	67^{10}	1	29 splits	

good ideal lattice codes for Bob's reliability. Note that the numerical computations are not obvious either, since they require units computations, which are lengthy, when the degree of the number fields increases. Examples of number fields can be found in Table 2, where we recall the smallest prime which is not inert, as computed in the previous section. We observe that maximal real subfields have very small regulators.

The case of degree 5 shows that the choice of the regulator is making a huge difference, since the dominant term for $U(q)$ is

$$\frac{2 \cdot 5^4}{4!R} (\log q)^4 = \frac{625}{12R} (\log q)^4$$

yielding respectively

$$\sim 0.4(\log q)^4, \quad \sim 32(\log q)^4$$

for the smallest (1.63 for $\mathbb{Q}(\zeta_{11})$) and biggest (93.768 for $\mathbb{Q}(\zeta_{61})$) regulators shown in Table 2.

Theorem 2 is an asymptotic result, holding for a region defined by q , when q grows to infinity. In our scenario, we are on the contrary interested in small regions, corresponding to the signal constellation transmitted. In order to get a sense of how valid it is to use this bound to evaluate the density of units in the regions considered, we computed (10) for $\mathcal{B}(6)$ for the number fields of degree 5 of Table 2. We observe that the regulator predicts very well which number field is giving the smallest sum even though the shaping region is simplified: when the regulator increases, the sum decreases. The difference between the smallest and biggest sum is also huge (roughly of a factor of 30), though not as huge as predicted (roughly of a factor of 80). Other experiments with other integral bases gave variations of the above results, but with the same overall behavior. Since the discriminants of the number fields considered are needed to normalize two lattices to have the same volume, the discriminants are also indicated in Table 3.

5 Conclusion and Future Work

This paper addresses the question of designing wiretap lattice codes for fast fading channels. First, we gave a clean upper bound on Eve's probability of correctly decoding the confidential message intended to Bob for finite constellations, which

allowed us to obtain a code design criterion to characterize the confusion that a lattice code induces for Eve. This code design is consistent with the one known for infinite constellations. Since ideal lattices are known to be suited for transmission between Alice and Bob over fast fading channels, we rewrite the code design criterion in terms of ideal lattices, which translates into a finite sum of inverse algebraic norms in number fields. The second part of this paper studies these sums of inverse norms. Elements of small norms have the biggest contributions to these sums. We first addressed the question of the role of elements of small norms to these sums of inverse norms. We proposed to consider number fields where small primes are inert, to prevent the existence of elements of small norms. We then consider the regulator of totally real subfields of cyclotomic fields, known to provide reliable ideal lattice codes. Current bounds on the regulator seem to characterize the behavior of the sum of inverse norms, even for small constellation sizes. This gives a first set of number fields candidate to provide good lattice wiretap codes.

The picture for wiretap lattice codes is however more complex, since it involves the design of not only Λ_e (the lattice designed to confuse Eve), but also Λ_b (the lattice that provides reliability for Bob). Though this has not been made completely explicit in this particular context of coset encoding, the discriminant d_K of the number field K is known [5, 1] to play a role in the design of Λ_b , and in fact, it is usually preferred to be not too big (this is on top of already knowing that the discriminant should not be too large since it is used for normalization). Table 3 illustrates how the discriminant d_K grows with the regulator. This suggests that the optimal design might be a trade-off between the discriminant and the regulator, and that further benefits in terms of confusion could be obtained by considering the ramification of small primes. This is a natural direction for further study.

References

1. E. Bayer-Fluckiger, F. Oggier, E. Viterbo, “Algebraic lattice constellations: Bounds on Performance”, *IEEE Transactions on Information Theory*, vol. 52, no. 1, 2006.
2. J.-C. Belfiore, F. Oggier, “Lattice Code Design for the Rayleigh Fading Wiretap Channel”, *Communications Workshops, International Conference on Communications (ICC 2011)*, Kyoto.
3. W. Ebeling, “Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch”, *Advanced Lectures in Mathematics*, Springer, 2013.
4. G.R. Everest and J.H. Loxton, “Counting Algebraic Units with Bounded Height”, *Journal of Number Theory*, 44, 1993.
5. X. Giraud, E. Boutillon, J.-C. Belfiore, “Algebraic tools to build modulation schemes for fading channels”, *IEEE Trans. on Information Theory*, vol. 43, no 3, 1997.
6. C. Hollanti and E. Viterbo, “Analysis on Wiretap Lattice Codes and Probability Bounds from Dedekind Zeta Functions”, *ICUMT 2011*, Hungary.
7. C. Hollanti, E. Viterbo and D.Karpuk “Nonasymptotic Probability Bounds for Fading Channels Exploiting Dedekind Zeta Functions”, preprint, arxiv.org/pdf/1303.3475
8. F. Lin and F. Oggier, “A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions”, *IEEE Transactions on Information Theory*, vol. 59, no. 6, June 2013. Available online at arxiv.org/pdf/1201.3688.
9. C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehlé, “Semantically Secure Lattice Codes for the Gaussian Wiretap Channel”, preprint, <http://arxiv.org/abs/1210.6673>
10. D.A. Marcus, “Number Fields”, Springer, 1977.
11. F. Oggier and E. Viterbo, “Algebraic number theory and code design for Rayleigh fading channels,” in *Foundations and Trends in Communications and Information Theory*, 2004, vol. 1, no. 3, pp. 333–415.

12. F. Oggier, P. Solé, J.-C. Belfiore, “Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis”, preprint, <http://arxiv.org/abs/1103.4086>
13. S.S. Ong, F. Oggier, “Lattices from Totally Real Number Fields with Large Regulator”, WCC 2013.
14. R. Vehkalahti, H.F. Lu, Lu, L. Luzzi, “Inverse Determinant Sums and Connections between Fading Channel Information Theory and Algebra”, *IEEE Transactions on Information Theory*, vol. 59, no. 9, Sept 2013. Available online at <http://arxiv.org/abs/1111.6289>