Title	Lattices from totally real number fields with large regulator
Author(s)	Ong, Soon Sheng; Oggier, Frédérique
Citation	Ong, S. S., & Oggier, F. (2013). Lattices from totally real number fields with large regulator. Proceedings of the International Workshop on Coding and Cryptography WCC 2013.
Date	2013
URL	http://hdl.handle.net/10220/24618
Rights	© 2013 Elsevier. This is the author created version of a work that has been peer reviewed and accepted for publication by Proceedings of International Workshop on Coding and Cryptography, Elsevier. 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://www.selmer.uib.no/WCC2013/pdfs/Ong.pdf].

Noname manuscript No.
(will be inserted by the editor)

Lattices from Totally Real Number Fields with Large Regulator

Soon Sheng Ong · Frédérique Oggier

Received: date / Accepted: date

Abstract We look for examples of totally real number fields with large regulator and inert small primes inside some families of cyclotomic fields. This problem is motivated by the design of wiretap codes for fast fading Rayleigh channels.

Keywords Lattices · Number Fields · Units

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 [11] and [8]) have been proposed as code design criteria for AWGN wiretap channels, in order to maximize the confusion at the eavesdropper, and lattice codes satisfying the former criterion have been studied [7].

In this paper, we focus on fast fading channels instead. A code design criterion to increase the eavesdropper confusion has been computed in [2], which involves the minimization of a sum of inverse norms in number fields.

The research of S.S. Ong and of F. Oggier for this work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.

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,frederique@ntu.edu.sg

This minimization has been addressed in [6] via the use of Dedekind zeta functions, and similar sums have been looked at in the context of the Diversity Multiplexing Trade-Offs (DMT) [12]. Here instead, we translate the problem of code design for fast fading channels into finding totally real number fields with large regulator and inert small primes.

We start by recalling the code design criterion for fast fading wiretap channels in Section 2, where we motivate the need for lattices coming from totally real number fields. We then look for totally real number fields with inert small primes within some families of cyclotomic fields in Section 3. In Section 4, we further find among these totally real number fields those with bigger regulator. Since this paper only focuses on the criterion to provide confusion at the eavesdropper, the last section lists other aspects that should be incorporated to finalize the design of wiretap codes for fast fading channels.

2 Coding for the Wiretap Rayleigh Fading Channel

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

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

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

$$\mathsf{diag}(\mathbf{h}_b) = \begin{pmatrix} |h_{b,1}| & & \\ & \ddots & \\ & & |h_{b,n}| \end{pmatrix}, \ \mathsf{diag}(\mathbf{h}_e) = \begin{pmatrix} |h_{e,1}| & & \\ & \ddots & \\ & & |h_{e,n}| \end{pmatrix} \tag{2}$$

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, $i = 1, \ldots, n$, 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.

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 we briefly recall now. 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, and for the actual transmission to happen, a point in this coset is chosen uniformly at random. The intuition behind this scheme is that coset encoding provides a labeling of the lattice points with a mixture of random and data bits. What it should achieve is to permit Eve to decode the random bits, but not the data bits, which is possible because of the difference of noises between the legitimate and the eavesdropper channel. The benefit of using lattice coset coding has been shown in [3] 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]. Once the fading is fixed, we deal with a Gaussian channel, and can use the results of [3]. The fading case is then obtained by averaging over the fading coefficients. The upper bound on Eve's probability of correct decision depends on parameters given by the channel, and by an expression that depends on the coding strategy, which is the part that can be optimized, leading to a design criterion: to minimize

$$\sum_{\mathbf{x}\in\Lambda_e,\mathbf{x}\neq 0} \prod_{x_i\neq 0} \frac{1}{|x_i|^3} \tag{3}$$

where $\mathbf{x} = (x_1, \ldots, x_n)$. A first observation is that it is desirable to have as many non-zero coefficients 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 $\mathbf{x}$, its *diversity* is the number of its non-zero coefficients. Given a lattice, its diversity is the minimum diversity over every non-zero lattice 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 $\sigma_1, \ldots, \sigma_{r_1}$ be the r_1 real embeddings of K, and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ 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 $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$, 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 $\sigma_1, \ldots, \sigma_n$.

Definition 1 An *ideal lattice* is an integral lattice $(\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an $\mathcal{O}_K$-ideal (which may be fractional) and

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

where $\alpha \in K$ 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.

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

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \ldots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix} \tag{4}$$

where $\alpha_j = \sigma_j(\alpha)$, for all j. One easily verifies that the Gram matrix MM^t is given by $\{\mathrm{Tr}(\alpha\, \omega_i \omega_j)\}_{i,j=1}^n$.

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

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

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, (3) becomes

$$\begin{aligned} \sum_{\mathbf{x}\in\Lambda_e, \mathbf{x}\neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3} &= \sum_{x \in \mathcal{I}, x \neq 0} \prod_{i=1}^n \frac{1}{\sqrt{\alpha_i}|\sigma_i(x)|^3} \\ &= \sum_{x \in \mathcal{I}, x \neq 0} \frac{1}{\sqrt{N_{K/\mathbb{Q}}(\alpha)}|N_{K/\mathbb{Q}}(x)|^3} \end{aligned} \tag{5}$$

since $\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^n u_i\omega_i \in \mathcal{I}$. In this paper, we will typically 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, $x \in \mathcal{I} = (\alpha)\mathcal{O}_K$, $N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(x')$ for some $x' \in \mathcal{O}_K$, and we see from (5) that the sum which becomes of interest is

$$\sum_{x \in \mathcal{O}_K, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}. \tag{6}$$

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 [10].

3 Some Number Fields with Prescribed Ramification

Let us make a first obvious remark regarding (6). 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 $r_2 = 1$).

The infinite sum (6) where $x \in \mathcal{O}_K$ comes from computing a probability of error over the whole lattice, instead of considering the actual signal constellation, which is a subset of it. A bound involving the whole lattice provides an upper bound on a finite constellation, and is often easier to handle, however, in this case, it is meaningful only for quadratic imaginary fields, and in general, the bound will have to involve a finite set of points:

$$\sum_{x \in \mathcal{O}_K \cap \mathcal{R}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}, \tag{7}$$

where $\mathcal{R}$ decides of the shape of the finite constellation.

3.1 Norms and Ramification

The dominant terms in this sum are integers with small norms. The contribution of the terms of norm 1 depends on the density of units, which we will discuss in Section 4, while that of elements of norm at least 2 depends on the ramification in K, the class number of K, 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).

Since the examples we will consider all have a class number of 1, and the density of units will be discussed in the next section, we next study the ramification effect.

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

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

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 pth 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 ramification in $\mathbb{Q}(\zeta_p)$ is well understood.

Theorem 1 *[9] Let q be a rational prime different from p, then q is unramified in $\mathbb{Q}(\zeta_p)$ and in fact*

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

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

$$e(\mathfrak{q}_L/q) = e(\mathfrak{q}_L/\mathfrak{q}_K)e(\mathfrak{q}_K/q), \; f(\mathfrak{q}_L/q) = f(\mathfrak{q}_L/\mathfrak{q}_K)f(\mathfrak{q}_K/q), \tag{8}$$

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 (8) 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 [1]: $q^2 \equiv 1 \pmod{p}$ is equivalent to $(q-1)(q+1) = 0 \pmod{p}$, 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 consider more generally a subfield K of $\mathbb{Q}(\zeta_p)$ of degree $[K : \mathbb{Q}] = m$, 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 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 (8)

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

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, 7, 11, 13, 17, 19 and 23 are inert. On the other hand, $29^3 \equiv 1 \pmod{67}$.

Among those totally real fields with inert small primes, we now look at those with small number of units, as considered next.

[1] We would like to thank the anonymous reviewer who proposed this simplification.

Table 1 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
$\mathbb{Q}(\zeta_{31})$	30.36	$x^5 - 9x^4 + 20x^3 - 5x^2 - 11x - 1$	5 splits
$\mathbb{Q}(\zeta_{41})$	123.32	$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$	3 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

4 Units and Regulator

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.

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

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

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 $\max_{1\le i\le d}|\sigma_i(u)| < q$ 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 $q \to \infty$ and $c = 6 \cdot 2 \cdot 10^{12} d^{10}(1 + 2\log d)$.

By choosing $\mathcal{R}$ accordingly, we might use this result on $U(q)$ to evaluate the amount of units, that is of elements of norm 1 in (7). 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 identified earlier. 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 1. We observe that though maximal real subfields have the advantage of having small primes under control, they also have very small regulators.

Table 2 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
$\mathbb{Q}(\zeta_{11})$	1.63	11^4	1	11 ramifies
$\mathbb{Q}(\zeta_{31})$	30.36	31^4	1	5 splits
$\mathbb{Q}(\zeta_{41})$	123.32	41^4	1	3 splits
$\mathbb{Q}(\zeta_{23})$	1014.31	23^{10}	1	23 ramifies
$\mathbb{Q}(\zeta_{67})$	330512.24	67^{10}	1	29 splits

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 and biggest regulators shown in Table 1.

In fact, this difference is so big that it might make irrelevant the consideration about the ramification of small primes. 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. Table 2 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.

5 Future Work

Identifying totally real number fields with prescribed ramification and regulator is only one step in the design of wiretap codes for fast fading channels, and the goal of this paper was to propose different number fields that could be used for that purpose, and to illustrate the trade-offs among the different parameters involved, taking into account solely the design of Λ_e, the lattice that provides confusion to the eavesdropper. Apart looking for more such fields inside cyclotomic fields with $\mathbb{Q}(\zeta_n)$, n not prime, and possibly among non-abelian Galois extensions, other criteria need to be understood:

– The design of wiretap codes involves the choice of both Λ_e and Λ_b, with $\Lambda_e \subset \Lambda_b$. It is needed to understand which ideal lattices can be built over

the number fields identified. For example, it is known that the integer lattice $\mathbb{Z}^{(p-1)/2}$ can be obtained on the ring of integers of the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with a suitable choice of α [10].
- The design of good lattices to ensure Bob's reliability needs to be taken into account (see [5] for a related work). In that case, the picture is more complicated, and is likely to involve the discriminant of the number field as well, yielding a trade-off between discriminant and regulator.
- Coset encoding in the context of ideal lattices needs to be addressed, in order to provide an efficient way of encoding (by performing a bit labeling of the lattice points).

These aforementioned items are different pieces of a puzzle, which need to be put together to obtain a fully working wiretap code, whose perform could be simulated.

Acknowledgements We would like to thank the anonymous reviewers for the useful comments.

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. F. Oggier, P. Solé, J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", preprint, `http://arxiv.org/abs/1103.4086`
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. F. Lin and F. Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions", *IEEE Transactions on Information Theory*, to appear, `arxiv.org/pdf/1201.3688`
8. 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`
9. D.A. Marcus, "Number Fields", *Springer*, 1977.
10. 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.
11. F. Oggier, P. Solé, J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel", preprint, `arxiv.org/pdf/1103.4086`
12. R. Vehkalahti, H.F. Lu, "Inverse Determinant Sums and Connections between Fading Channel Information Theory and Algebra", preprint, `http://arxiv.org/abs/1111.6289`