An analysis of small dimensional fading wiretap lattice codes

Ducoat, Jérôme; Oggier, Frédérique

2014

Ducoat, J., & Oggier, F. (2014). An analysis of small dimensional fading wiretap lattice codes. 2014 IEEE International Symposium on Information Theory (ISIT), 966-970.

<https://hdl.handle.net/10356/103868>

<https://doi.org/10.1109/ISIT.2014.6874976>

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/ISIT.2014.6874976>].

Downloaded on 26 Apr 2023 20:07:33 SGT

An Analysis of Small Dimensional Fading Wiretap Lattice Codes

Jérôme Ducoat and Frédérique Oggier

Division of Mathematical Sciences

Nanyang Technological University

Singapore

Email: jducoat@ntu.edu.sg, frederique@ntu.edu.sg

Abstract—We consider sums of inverse of algebraic norms as a code design criterion for fading wiretap channels. We study their behavior for small dimensional lattices built over the ring of integers of a number field, where the lattice points are taken from finite constellations, whose shaping is either cubic or spheric. Our analysis shows that unimodular lattices whose underlying number field has a small discriminant give the best performance so far.

I. INTRODUCTION

Wiretap codes are codes that promise both reliability and confidentiality over noisy communication channels, in the presence of an eavesdropper. They have been shown to exist for a variety of channels, though explicit constructions remain sparse (see [1] for a survey including wiretap codes built from classical error correcting codes, polar codes and lattices, and [2] for wiretap codes built from LDPC codes). While the notion of confidentiality for wiretap codes is usually captured by the mean of mutual information (or equivocation), some recent works have tried to propose other measures, such as the secrecy gain [4], based on the eavesdropper's probability $P_{c,e}$ of being able to correctly decode, or the flatness factor [5], both for Gaussian channels.

A bound on the eavesdropper's probability $P_{c,e}$ of correct decoding has been computed for fading channels [6]. Since lattice constellations coming from number fields are known to provide reliability for fading channels [7], this bound on $P_{c,e}$ has been refined for this specific case, leading to a code design criterion for confidentiality, which consists of minimizing a sum of inverse of algebraic norms of the form

$$\sum_{\substack{x \in \mathcal{O}_K \cap \iota^{-1}(\mathcal{R}) \\ x \neq 0}} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3} \quad (1)$$

where K is a number field, $\mathcal{O}_K$ its ring of integers, and $\iota^{-1}(\mathcal{R})$ a finite region around the origin to be computed next.

The study of sums of inverse of algebraic norms of the form (1) appeared in [8], in fact more generally, involving division algebras over number fields, in the context of the Diversity Multiplexing Trade-off (DMT). In the setting of wiretap fading channels, the connection between sums of inverse of algebraic norms and the Dedekind zeta function (which is a sum of inverse of ideal norms) has been investigated in [9], [10]. Number fields with no (non-unit) element of small algebraic

norms have been looked at in [11]. From a purely number theoretic point of view, the number of units in a large region around the origin has been bounded in [12]. This plays a role here, since units have norm 1, and are thus contributing the heaviest weight in (1). The findings regarding (1) so far are that asymptotically, the units, and thus in turn the regulator of K [8], [12] play a big role in the behavior of the sum.

In this paper, we are interested in (1) in a non-asymptotic regime, taking into account the lattice obtained once given a number field K , which in particular includes the volume of the lattice but also its shaping once a finite region $\mathcal{R}$ is fixed. The region $\mathcal{R}$ is chosen to be either a hypercube fitted with coordinate axes or with the lattice axes, in order to obtain a cubic shaping, or a hypersphere. In Section II, we summarize the background on code design for fading wiretap codes and lattices built from number fields. In Section III, we explain our methodology, including the lattice shaping, and illustrate it with quadratic fields, which provide a visual intuition. However, since lattice codes are more interesting when the dimension grows, quartic and octic fields are considered next in Section IV. The main conclusions of our analysis so far are that:

- 1) unimodular ideal lattices tend to have smaller sums,
- 2) among unimodular lattices, the smaller the discriminant is, the smaller the sum will be.

II. WIRETAP FADING CHANNELS

We consider communication over a wiretap channel, where a legitimate user Alice sends information to another legitimate user Bob, 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

$$\mathbf{y} = \text{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b, \quad \mathbf{z} = \text{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e, \quad (2)$$

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 $\text{diag}(\mathbf{h}_b) = \text{diag}(|h_{b,1}|, \dots, |h_{b,n}|)$, $\text{diag}(\mathbf{h}_e) = \text{diag}(|h_{e,1}|, \dots, |h_{e,n}|)$ 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. $\sigma_{h,e}^2$.

Alice sends a lattice point $\mathbf{x} \in \Lambda_b \subset \mathbb{R}^n$. To confuse Eve, she uses the standard coset coding technique: 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, a point $\mathbf{c} + \mathbf{r}$ in this coset is chosen uniformly at random.

A. A Code Design Criterion

A measure of the confusion that coset coding causes, given a sublattice Λ_e , is Eve's average probability $\bar{P}_{c,e}$ of correct decision [6], which is upper bounded by

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

where $\text{vol}(\Lambda_b)$ is the volume of Λ_b , and $\mathcal{R}$ is the region that shapes the finite constellation. This motivated the following design criterion for fast fading wiretap codes: to minimize

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

where $\mathbf{x} = (x_1, \dots, x_n)$. It is desirable that all the non-zero vectors $\mathbf{x} \in \Lambda_e$ have only non-zero coefficients. This property happens to be the same as needed to ensure Bob's reliability [7], that of maximizing the lattice *diversity*. 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. We say *full diversity* when the diversity is n .

We thus assume that the lattice Λ_b is fully diverse, this in turn forces the sublattice Λ_e to be fully diverse, in which case the wiretap code design criterion becomes to minimize

$$\sum_{\mathbf{x} \in \Lambda_e \cap \mathcal{R}, \mathbf{x} \neq 0} \prod_{i=1}^n \frac{1}{|x_i|^3}. \quad (4)$$

It may be counterintuitive that full diversity, which implies reliability for Bob, should help confusion for Eve. This happens because ideally, one would like Eve to actually reliably decode only the random bits sent by Alice. In other words, full diversity does help to minimize (4).

B. Ideal Lattices

The property of full diversity is well understood in the context of *ideal lattices* [7]. Let K be a totally real number field of degree n . Let $\sigma_1, \dots, \sigma_n$ be the n real embeddings of K (i.e., field homomorphisms from K to $\mathbb{R}$). An *ideal lattice* is a lattice $\Lambda = (\mathcal{I}, q_\alpha)$, where $\mathcal{I}$ is an ideal of the ring of integers $\mathcal{O}_K$ of K and

$$\begin{aligned} q_\alpha : \mathcal{I} \times \mathcal{I} &\rightarrow \mathbb{Z} \\ (x, y) &\mapsto \text{Tr}_{K/\mathbb{Q}}(\alpha xy) \end{aligned}$$

where $\alpha \in K$ is a totally positive element (i.e., for every $i \in \{1, \dots, n\}$, $\alpha_i = \sigma_i(\alpha) > 0$) of the codifferent ideal $\mathcal{D}_{K/\mathbb{Q}}^{-1}$.

The condition that α is in the codifferent ideal ensures that the lattice is integral. Given a $\mathbb{Z}$ -basis $\{\omega_1, \dots, \omega_n\}$ of the ideal $\mathcal{I}$, the generator matrix of the ideal lattice $(\mathcal{I}, q_\alpha)$ is

$$A = \begin{pmatrix} \sqrt{\alpha_1} \sigma_1(\omega_1) & \sqrt{\alpha_2} \sigma_2(\omega_1) & \cdots & \sqrt{\alpha_n} \sigma_n(\omega_1) \\ \vdots & \vdots & \cdots & \vdots \\ \sqrt{\alpha_1} \sigma_1(\omega_n) & \sqrt{\alpha_2} \sigma_2(\omega_n) & \cdots & \sqrt{\alpha_n} \sigma_n(\omega_n) \end{pmatrix}.$$

We can derive how the ideal $\mathcal{I}$ can be seen as a real lattice :

$$\begin{aligned} \iota : \mathcal{I} &\rightarrow \mathbb{R}^n \\ x &= \sum_{i=1}^n \lambda_i \omega_i \mapsto \mathbf{x} = (\sqrt{\alpha_1} \sigma_1(x), \dots, \sqrt{\alpha_n} \sigma_n(x)) \end{aligned}$$

Since, for all $x \in \mathcal{I} \setminus \{0\}$ and all $1 \leq i \leq n$, $\sqrt{\alpha_i} \sigma_i(x) \neq 0$, the ideal lattices are always fully diverse when coming from a totally real number field K . Moreover, in the context of ideal lattices, the simplified confidentiality design criterion (3) can be re-expressed in terms of the algebraic norm as follows :

$$\frac{1}{(\sqrt{N_{K/\mathbb{Q}}(\alpha)})^3} \sum_{\substack{x \in \mathcal{I} \cap \iota^{-1}(\mathcal{R}) \\ x \neq 0}} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}. \quad (5)$$

III. METHODOLOGY AND QUADRATIC FIELDS

In the sequel, we focus on the ideal lattices where $\mathcal{I} = \mathcal{O}_K$. This choice is justified by the fact that in the case of number fields with class number 1, for every $\beta \in \mathcal{O}_K$, the ideal lattice $((\beta), \alpha)$ is equal to $(\mathcal{O}_K, \alpha\beta^2)$. Moreover, since we will be considering fields with small discriminants, most of these number fields have class number 1.

We want to compare the sums (5) among number fields of fixed dimension (2, 4 and 8 in our case) and also using different choices of a shaping region $\mathcal{R}$.

A. General Methodology

In order to make the comparison suitable, we consider lattices with fixed volume. The volume of an ideal lattice $\Lambda = (\mathcal{O}_K, q_\alpha)$ is given by

$$\text{vol}(\Lambda) = |\det(A)| = \sqrt{N_{K/\mathbb{Q}}(\alpha) |D_K|},$$

where D_K denotes the discriminant of the number field K . Hence, we can look for totally positive elements α , so that the volume is 1 (if such a α exists in $\mathcal{D}_{K/\mathbb{Q}}^{-1}$, the lattice is called *unimodular*). Therefore, an ideal lattice is unimodular if and only if there exists a totally positive element $\alpha \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ such that $N_{K/\mathbb{Q}}(\alpha) = \frac{1}{|D_K|}$.

In small dimensions ($n < 8$), there is, up to equivalence, only one unimodular lattice, namely the cubic lattice $\mathbb{Z}^n$. We first compare among ideal lattices which are equivalent to $\mathbb{Z}^n$. For such lattices, we will consider three different shapings $\mathcal{R}$:

- 1) the hypercube fitted with the coordinate axes, denoted by $\mathcal{R}_1$
- 2) the hypersphere, denoted by $\mathcal{R}_2$
- 3) the hypercube fitted with the lattice axis, denoted by $\mathcal{R}_3$.

All three regions have been chosen since they are energy efficient, though $\mathcal{R}_3$ provides a more practical bit labeling.

Fig. 1: Parallelopete and preimage $(\tilde{\iota})^{-1}(\mathcal{R}_1)$, where $\mathcal{R}_1$ has size 6 and $K = \mathbb{Q}(\sqrt{13})$.

The advantage of the shapings $\mathcal{R}_1$ and $\mathcal{R}_2$ is that we are comparing sums over points within the same area among the different lattices (unimodular or not). However, it is not easy to predict the number of lattice points there will be inside the regions $\mathcal{R}_1$ and $\mathcal{R}_2$. The advantage of considering $\mathcal{R}_2$ and $\mathcal{R}_3$ is that, in each case, the number of points will be constant among the different field extensions (and completely known for $\mathcal{R}_3$), which allows a fair comparison. Lastly, the shaping $\mathcal{R}_3$ is more convenient for the lattices isomorphic to $\mathbb{Z}^n$. For other lattices, the equivalent shaping will depend on the fundamental region of the lattice.

Once we have determined the shaping $\mathcal{R}$, we want to find in $\mathcal{O}_K$ the elements whose image by ι belongs to $\mathcal{R}$. It is well known that $\mathcal{O}_K$ is a free $\mathbb{Z}$ -module with rank n , so ι yields the following $\mathbb{Z}$ -linear map :

$$\tilde{\iota} : (\lambda_1, \dots, \lambda_n) \mapsto x = \sum_{1 \leq j \leq n} \lambda_j \omega_j \mapsto \iota(x).$$

Finding the elements of $\mathcal{O}_K \cap \iota^{-1}(\mathcal{R})$ is then equivalent to find the points with integer coefficients (*integral points*) in $(\tilde{\iota})^{-1}(\mathcal{R})$. Let us work out the case of the hypercube $\mathcal{R}_1$. Then $(\tilde{\iota})^{-1}(\mathcal{R})$ is a parallelopete and we want to enumerate the integral points inside. One way to do so is to inscribe this parallelopete in a hypercube and then test on all integral points of the hypercube (which are easily enumerated) whether they belong to $(\tilde{\iota})^{-1}(\mathcal{R})$. However, as we increase the dimension (already for dimension 8), computations become very lengthy. One way to speed up the enumeration process is to split the n -dimensional spaces in 2^n *coordinate orthants* (intersection of n different coordinate half-spaces) and then fit the hypercube to the intersection of the parallelopete with the orthant as shown in Figure 1. Moreover, if $x \in \mathcal{O}_K \cap \iota^{-1}(\mathcal{R})$, then it is easily seen that $-x \in \mathcal{O}_K \cap \iota^{-1}(\mathcal{R})$ since $\iota(-x) = -\iota(x)$ and that $|N_{K/\mathbb{Q}}(-x)| = |N_{K/\mathbb{Q}}(x)|$. We then need to focus on a half-space only.

B. Quadratic Fields

Let d be a squarefree positive integer and let $K = \mathbb{Q}(\sqrt{d})$. As mentioned above, there is only one unimodular lattice in dimension 2 (up to isomorphism). We first determine when the ideal lattice $(\mathcal{O}_K, \alpha)$ is isomorphic to $\mathbb{Z}^2$.

Fact 1 : There exists $\beta \in K$ such that $|D_K| = N_{K/\mathbb{Q}}(\beta)$ if and only if there exists $u \in K$ such that $N_{K/\mathbb{Q}}(u) = -1$. In this case, we can always find a totally positive element with norm $|D_K|$.

Proof: If $d \equiv 1 \pmod{4}$, $|D_K| = d$ and $N_{K/\mathbb{Q}}(\sqrt{d}) = -d = -|D_K|$. If $d \not\equiv 1 \pmod{4}$, $|D_K| = 4d$ and $N_{K/\mathbb{Q}}(2\sqrt{d}) = -4d = -|D_K|$. The equivalence is immediate. Moreover, if $\beta \in K$ is such that $\sigma_1(\beta)\sigma_2(\beta) = N_{K/\mathbb{Q}}(\beta) = |D_K|$, then $\sigma_1(\beta)$ and $\sigma_2(\beta)$ have the same sign. If they are both negative, $-\beta$ is totally positive and has norm $|D_K|$. ■

The equivalence in Fact 1 is in particular satisfied when $d \equiv 1 \pmod{4}$ and d is prime ([13], Corollary 2, p. 182). Note that these quadratic fields are not the only ones that have this property. Indeed, in $\mathbb{Q}(\sqrt{2})$, $1 + \sqrt{2}$ has norm -1 .

Assume that the equivalence in Fact 1 is satisfied. Then the ideal lattice is a rotated square lattice.

Example 1: Fix $K = \mathbb{Q}(\sqrt{13})$. The element $\alpha = \frac{1}{2} + \frac{3}{26}\sqrt{13}$ is totally positive and has algebraic norm 13. As before, we denote by ι the embedding from $\mathcal{O}_K$ to $\mathbb{R}^2$. An integral basis of K is $(\frac{1+\sqrt{13}}{2}, \sqrt{13})$. In Figure 2, we draw the image of these two vectors via ι . For the three different shaping regions $\mathcal{R}$, we represented the lattice points inside $\mathcal{R}$ (as squares for the images of units in $\mathcal{O}_K$, as circles for the others). We can note for instance that the number of units is dependent on the shaping.

In Table I, we give some results in dimension 2 for the totally real quadratic fields with smallest discriminant. In particular, we can note that the best example for minimizing the sum and the discriminant together is given by the extension with the smallest discriminant, independently of the shaping. We also note that the discriminant is not giving an exact rule for minimizing the sum (5) : for instance, the number fields $\mathbb{Q}(\sqrt{37})$ and $\mathbb{Q}(\sqrt{10})$, which have discriminant 37 and 40 respectively give bigger sums for the shaping $\mathcal{R}_3$ with length 200 than the number field $\mathbb{Q}(\sqrt{41})$.

In the non-unimodular case, we cannot make the ideal lattice to have volume 1 by twisting the trace form. To allow a fair comparison with the unimodular lattices, we rescale our results by multiplying by the volume of the lattice $\sqrt{|D_K|}$.

Example 2: Let $K = \mathbb{Q}(\sqrt{3})$. Then $(1, \sqrt{3})$ is an integral basis of K . As stated earlier, the volume of the ideal lattice $(\mathcal{O}_K, 1)$ is equal to $2\sqrt{3}$. For the shaping $\mathcal{R}_1$ with length 200, the sum is equal to 678.0, the number of units is 14 and there are 11551 lattice points inside $\mathcal{R}_1$. With normalization, we obtain that the sum is 2348.7, the number of units becomes approximately 48.5 and the number of points becomes 40013.8.

In Table II, we give the values of the sums for the totally real number fields with smallest discriminants and which do not yield unimodular lattices. We note that the values of the sums that we obtain are much bigger than for unimodular lattices.

IV. QUARTIC AND OCTIC FIELDS

We apply here the same procedure. We first want to decide whether the ideal lattice is unimodular.

Fact 2 : There exists $\beta \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ with norm $\pm D_K$ if and only

Fig. 2: The 3 different shapings for length/diameter 6 and $K = \mathbb{Q}(\sqrt{13})$

K	h_K	D_K	R_K	Shaping $\mathcal{R}_1$			Shaping $\mathcal{R}_2$			Shaping $\mathcal{R}_3$		
				Sum (5)	Units	Points in $\mathcal{R}_1$	Sum (5)	Units	Points in $\mathcal{R}_2$	Sum (5)	Units	Points in $\mathcal{R}_3$
$\mathbb{Q}(\sqrt{5})$	1	5	0.48	458.1	40	40001	458.1	40	31417	502.9	44	40401
$\mathbb{Q}(\sqrt{2})$	1	8	0.88	611.4	24	40001	611.4	24	31417	622.7	24	40401
$\mathbb{Q}(\sqrt{13})$	1	13	1.19	821.7	16	39997	821.7	16	31417	821.9	16	40401
$\mathbb{Q}(\sqrt{17})$	1	17	2.09	1049.8	12	40001	1049.8	12	31417	1050.5	12	40401
$\mathbb{Q}(\sqrt{29})$	1	29	1.65	1945.0	12	40005	1945.0	12	31417	1945.0	12	40401
$\mathbb{Q}(\sqrt{37})$	1	37	2.49	1985.6	8	40001	1985.6	8	31417	2019.7	8	40401
$\mathbb{Q}(\sqrt{10})$	2	40	1.82	3121.8	12	39993	3121.8	12	31417	3121.8	12	40401
$\mathbb{Q}(\sqrt{41})$	1	41	4.16	1535.7	4	40001	1535.7	4	31417	1536.0	4	40401

TABLE I: Sums in dimension 2 for shapes of length/diameter 200, unimodular lattices.

K	h_K	D_K	R_K	Shaping $\mathcal{R}_1$			Shaping $\mathcal{R}_2$		
				Norm. Sum	Norm. Units	Norm. Points in $\mathcal{R}_1$	Norm. Sum	Norm. Units	Norm. Points in $\mathcal{R}_2$
$\mathbb{Q}(\sqrt{3})$	1	12	1.32	2348.7	48.5	40013.8	2348.7	48.5	31388.2
$\mathbb{Q}(\sqrt{6})$	1	24	2.29	6662.1	49.0	40019.8	6662.1	49.0	31397.6
$\mathbb{Q}(\sqrt{7})$	1	28	2.77	6001.0	31.7	40019.6	6001.0	31.7	31394.5

TABLE II: Sums in dimension 2 for shapes of length/diameter 200, non-unimodular lattices.

K	h_K	D_K	R_K	Shaping $\mathcal{R}_1$			Shaping $\mathcal{R}_2$			Shaping $\mathcal{R}_3$		
				Sum (5)	Units	Points in $\mathcal{R}_1$	Sum (5)	Units	Points in $\mathcal{R}_2$	Sum (5)	Units	Points in $\mathcal{R}_3$
K_1	1	725	0.83	$7.27 \cdot 10^6$	372	10013	$6.41 \cdot 10^6$	328	3121	$1.07 \cdot 10^7$	548	14641
K_2	1	1125	1.17	$1.08 \cdot 10^7$	284	9997	$9.41 \cdot 10^6$	248	3121	$1.52 \cdot 10^7$	400	14641
K_3	1	1600	1.54	$1.48 \cdot 10^7$	228	10001	$1.32 \cdot 10^7$	204	3121	$1.99 \cdot 10^7$	308	14641
K_4	1	1957	1.92	$1.62 \cdot 10^7$	182	10005	$1.42 \cdot 10^7$	160	3121	$2.28 \cdot 10^7$	256	14641
K_5	1	2000	1.85	$1.67 \cdot 10^7$	184	10013	$1.56 \cdot 10^7$	172	3121	$2.26 \cdot 10^7$	248	14641
K_6	1	2048	2.44	$1.50 \cdot 10^7$	244	9993	$1.31 \cdot 10^7$	128	3121	$2.15 \cdot 10^7$	208	14641

TABLE III: Sums in dimension 4 for shapes of length/diameter 10, unimodular lattices.

K	h_K	D_K	R_K	Lattice	Shaping $\mathcal{R}_1$			Shaping $\mathcal{R}_3$		
					Sum (5)	Units	Points in $\mathcal{R}_1$	Sum (5)	Units	Points in $\mathcal{R}_3$
L_1	1	282300416	22.45	E_8	$7.59 \cdot 10^{14}$	160	249			
L_2	1	309593125	23.70	Non-unimodular	$1.26 \cdot 10^{15}$	230.6	319.1			
L_3	1	324000000	24.39	$\mathbb{Z}^8$	$8.40 \cdot 10^{14}$	144	289	$1.20 \cdot 10^{16}$	2056	6561
L_4	1	410338673	28.44	$\mathbb{Z}^8$	$1.20 \cdot 10^{15}$	144	241	$1.60 \cdot 10^{16}$	1920	6561
L_5	1	432640000	28.99	E_8	$1.37 \cdot 10^{15}$	152	241			

TABLE IV: Sums in dimension 8 for shapes of length/diameter 2

if the ideal norm of the conductor of the number field is the algebraic norm of an element of K .

Proof: Let θ be a primitive element of K , let f be the minimal polynomial of θ and let f' denote its formal derivative. Let also $\mathcal{D}_{K/\mathbb{Q}}$ be the different ideal of $\mathcal{O}_K$ and let $\mathfrak{f}$ be the conductor of the field. We recall here that $\mathfrak{f} = \{x \in K | x\mathcal{O}_K \subset \mathbb{Z}[\theta]\}$. As stated in [3], Theorem III.2.5, we have $f'(\theta)\mathcal{O}_K = \mathfrak{f}\mathcal{D}_{K/\mathbb{Q}}$, so by taking the norms, we get that $|N_{K/\mathbb{Q}}(f'(\theta))| = N(\mathfrak{f})|D_K|$. ■

This equivalence in Fact 2 is satisfied when the conductor $\mathfrak{f}$ is a principal ideal and a fortiori when the class number h_K of K is 1.

Fact 3 : Assume that the equivalence in Fact 2 is satisfied. There exists $\alpha \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ totally positive and with algebraic norm $|D_K|$ if and only if there exists a unit u whose image via ι belongs to the same coordinate orthant than β . Moreover, if such a u exists, it can be found in the list of all the products of fundamental units and -1 (without powers).

Proof: Let $\beta \in \mathcal{D}_{K/\mathbb{Q}}^{-1}$ with norm $\pm D_K$. Let $u \in \mathcal{O}_K$ be a unit. For all $1 \leq i \leq n$, we have $\sigma_i(u\beta) = \sigma_i(u)\sigma_i(\beta)$, which is positive if and only if $\sigma_i(u)$ and $\sigma_i(\beta)$ have the same sign. Moreover, if such a u exists, $|N_{K/\mathbb{Q}}(u\beta)| = |N_{K/\mathbb{Q}}(u)| \cdot |N_{K/\mathbb{Q}}(\beta)| = |D_K|$ and

$$N_{K/\mathbb{Q}}(u\beta) = \prod_{1 \leq i \leq n} \sigma_i(u\beta) > 0.$$

Assume now that such a u exists. Then if $u_1, \dots, u_{n-1}$ denote the fundamental units of K , we can write $u = \pm u_1^{m_1} \dots u_{n-1}^{m_{n-1}}$ and, for all $1 \leq i \leq n$, $\sigma_i(u) = \pm \sigma_i(u_1)^{r_1} \dots \sigma_i(u_{n-1})^{r_{n-1}}$. Therefore, the sign of $\sigma_i(u)$ is the same as the sign of the product $\pm \sigma_i(u_1)^{r_1} \dots \sigma_i(u_{n-1})^{r_{n-1}}$, where r_j is the remainder of n_j by the euclidean division by 2 for all $1 \leq j \leq n-1$. We can then replace u with $v = \pm u_1^{r_1} \dots u_{n-1}^{r_{n-1}}$. ■

We give in Table III the values of the sums for unimodular lattices in dimension 4, for the 6 ideal lattices with smallest discriminants. The associated number fields $K_1, \dots, K_6$ are respectively defined by the following minimal polynomials : $y^4 - y^3 - 3y^2 + y + 1$, $y^4 - y^3 - 4y^2 + 4y + 1$, $y^4 - 6y^2 + 4$, $y^4 - 4y^2 - y + 1$, $y^4 - 5y^2 + 5$, $y^4 - 4y^2 + 2$. Once again, we note that the discriminant seems to give the behaviour of the sum (5) and to be more important than the regulator. Note that the first non-unimodular lattice in dimension 4 with small discriminant is given by $y^4 - 7y^2 + 11$ and discriminant 4400. The sum for this number field with shaping $\mathcal{R}_1$ and length 20 is equal to $5.88 \cdot 10^7$ and is much bigger than for number fields with comparable discriminant in the unimodular case.

In dimension 8, there are two isomorphism classes of unimodular lattices : namely, the class of the cubic lattice $\mathbb{Z}^8$ and the class of the lattice E_8 . In order to decide whether the ideal lattice is $\mathbb{Z}^8$ or E_8 , we check if the lattice is even or odd (we say that a unimodular lattice $(\mathcal{O}_K, q_\alpha)$ is even if, for all $x \in \mathcal{O}_K$, $q_\alpha(x, x)$ is even; it is said to be odd otherwise).

Fact 4: $(\mathcal{O}_K, q_\alpha)$ is even if and only if, for all $1 \leq i \leq n$, $q_\alpha(\omega_i, \omega_i)$ is even.

Proof: It follows from the fact that, if $x = \sum_{1 \leq i \leq n} \lambda_i \omega_i$,

$$q_\alpha(x, x) = \sum_{1 \leq i \leq n} q_\alpha(\omega_i, \omega_i) + 2 \sum_{1 \leq i < j \leq n} \text{Tr}_{K/\mathbb{Q}}(\alpha \omega_i \omega_j).$$

■

In Table IV, we studied the ideal lattices given by the number fields $L_1, \dots, L_5$ defined respectively by the following minimal polynomial : $y^8 - 4y^7 + 14y^5 - 8y^4 - 12y^3 + 7y^2 + 2y - 1$, $y^8 - 4y^7 - y^6 + 17y^5 - 5y^4 - 23y^3 + 6y^2 + 9y - 1$, $y^8 - 7y^6 + 14y^4 - 8y^2 + 1$, $y^8 - y^7 - 7y^6 + 6y^5 + 15y^4 - 10y^3 - 10y^2 + 4y + 1$ and $y^8 - 2y^7 - 7y^6 + 16y^5 + 4y^4 - 18y^3 + 2y^2 + 4y - 1$. These fields have the smallest discriminants in dimension 8.

Regarding the number field L_2 , since only the zero vector was inside the shaping $\mathcal{R}_1$ with length 2 (denoted by $\mathcal{R}_1(2)$), we considered instead the shaping $\mathcal{R}_1$ with length 6 (denoted by $\mathcal{R}_1(6)$), containing 119 lattice points and normalized accordingly by multiplying by $\frac{\sqrt{D_K} \cdot \text{vol}(\mathcal{R}_1(2))}{\text{vol}(\mathcal{R}_1(6))}$. The values of the sums for the different shapings confirm the trend that unimodular lattices yield smaller sums and that the variations between discriminants are fitting with the sums (5).

ACKNOWLEDGEMENT

The authors would like to warmly thank P. Purkayastha and E. Niaf for their help in speeding up the computations. The research of J. Ducoat and F. Oggier for this work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.

REFERENCES

- [1] F. Lin and F. Oggier, "Coding for wiretap channels", in *Physical Layer Security in Wireless Communications*, Auerbach Publications, CRC Press, Taylor&Francis Group.
- [2] D. Kline, J. Ha, S. McLaughlin, J. Barros, B.-J. Kwak, "LDPC Codes for the Gaussian Wiretap Channel", in *Physical Layer Security in Wireless Communications*, Auerbach Publications, CRC Press, Taylor&Francis Group.
- [3] J. Neukirch, "Algebraic Number Theory", Series: Grundlehren der mathematischen Wissenschaften, Vol. 322, 1999
- [4] F. Oggier, P. Sol, J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", preprint, available at <http://arxiv.org/abs/1103.4086>
- [5] C. Ling, L. Luzzi, J.-C.-Belfiore, D. Stehle, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", preprint, available at <http://arxiv.org/abs/1210.6673>
- [6] J.-C. Belfiore, F. Oggier, "Lattice Code Design for the Rayleigh Fading Wiretap Channel", *Communications Workshops, International Conference on Communications (ICC 2011)*, Kyoto.
- [7] 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.
- [8] R. Vehkalahti, H.F. Lu, "Inverse Determinant Sums and Connections between Fading Channel Information Theory and Algebra", *IEEE Trans. on Information Theory*, vol. 59, no 9, Sept 2013, available at <http://arxiv.org/abs/1111.6289>
- [9] C. Hollanti and E. Viterbo, Analysis on Wiretap Lattice Codes and Probability Bounds from Dedekind Zeta Functions, ICUMT 2011, Hungary.
- [10] 7. C. Hollanti, E. Viterbo and D. Karpuk, Nonasymptotic Probability Bounds for Fading Channels Exploiting Dedekind Zeta Functions, preprint, arxiv.org/pdf/1303.3475
- [11] S.S. Ong, F. Oggier, "Lattices from Totally Real Number Fields with Large Regulator", WCC 2013.
- [12] G.R. Everest and J.H. Loxton, "Counting Algebraic Units with Bounded Height", *Journal of Number Theory*, 44, 1993.
- [13] A. Fröhlich, M. J. Taylor, *Algebraic Number Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1991.