Probability Bounds for Two-Dimensional Algebraic Lattice Codes

David Karpuk

Aalto University

April 16, 2013

(Joint work with C. Hollanti and E. Viterbo)

Alice, Bob, and Eve

Suppose that Alice wants to transmit information to Bob over a potentially noisy wireless channel, while an eavesdropper, (St)Eve, listens in.

— — — — ∗ ∗ ∗ ∗ — — — —— >>

|

∗

|

Alice, Bob, and Eve

This wireless channel can be modeled by the equations

$$y_b = H_b x + z_b \tag{1}$$

$$y_e = H_e x + z_e \tag{2}$$

where

- $x \in \mathbf{R}^n$ is the vector intended for transmission.

Alice, Bob, and Eve

This wireless channel can be modeled by the equations

$$y_b = H_b x + z_b \tag{1}$$
$$y_e = H_e x + z_e \tag{2}$$

where

- $x \in \mathbf{R}^n$ is the vector intended for transmission.
- $H_b, H_e \in M_n(\mathbf{R})$ are Bob's and Eve's fading matrices, respectively.

Alice, Bob, and Eve

This wireless channel can be modeled by the equations

$$y_b = H_b x + z_b \tag{1}$$
$$y_e = H_e x + z_e \tag{2}$$

where

- $x \in \mathbf{R}^n$ is the vector intended for transmission.
- $H_b, H_e \in M_n(\mathbf{R})$ are Bob's and Eve's fading matrices, respectively.
- $z_b, z_e \in \mathbf{R}^n$ are the corresponding noise vectors, whose entries are Gaussian random variables with variance σ_b^2, σ_e^2.

Alice, Bob, and Eve

This wireless channel can be modeled by the equations

$$y_b = H_b x + z_b \tag{1}$$

$$y_e = H_e x + z_e \tag{2}$$

where

- $x \in \mathbf{R}^n$ is the vector intended for transmission.
- $H_b, H_e \in M_n(\mathbf{R})$ are Bob's and Eve's fading matrices, respectively.
- $z_b, z_e \in \mathbf{R}^n$ are the corresponding noise vectors, whose entries are Gaussian random variables with variance σ_b^2, σ_e^2.
- $y_b, y_e \in \mathbf{R}^n$ are the vectors received by Bob and Eve.

Alice, Bob, and Eve

This wireless channel can be modeled by the equations

$$y_b = H_b x + z_b \tag{1}$$
$$y_e = H_e x + z_e \tag{2}$$

where

- $x \in \mathbf{R}^n$ is the vector intended for transmission.
- $H_b, H_e \in M_n(\mathbf{R})$ are Bob's and Eve's fading matrices, respectively.
- $z_b, z_e \in \mathbf{R}^n$ are the corresponding noise vectors, whose entries are Gaussian random variables with variance σ_b^2, σ_e^2.
- $y_b, y_e \in \mathbf{R}^n$ are the vectors received by Bob and Eve.

We assume that $\sigma_e^2 >> \sigma_b^2$, i.e. that Eve's channel is much noisier than Bob's.

Coset Coding

Alice uses *coset coding*, a variant of lattice coding, to confuse Eve.

Alice selects a "fine" lattice Λ_b whose elements encode data intended for Bob. At the same time, Alice chooses a "coarse" sublattice

$$\Lambda_e \subset \Lambda_b, \tag{3}$$

containing random bits intended to confuse Eve.

Coset Coding

Alice now sends codewords of the form

$$x = r + c \tag{4}$$

where r is a random element of Λ_e intended to confuse Eve, and c is a coset representative of Λ_e in Λ_b.

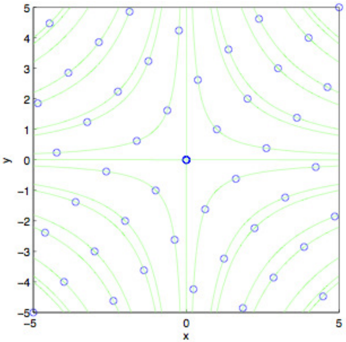
Alice's strategy ensures that Eve can easily recover the "random" data r, but not the actual data c.

Coset Coding

In practice, we construct Eve's codebook from a finite subset $\mathcal{C}_R$ of Λ_e, which we'll define as

$$\mathcal{C}_R := \{x \in \Lambda_e : ||x||_\infty \leq R\} \tag{5}$$

for some positive $R > 0$. In this picture, the blue dots represent elements of Λ_e, and $R = 5$:



Probability of Eve's Correct Decision

Given the above scheme to be employed by Alice, what is the probability that Eve correctly decodes the data c? It is known that this probability can be estimated by

$$P_e \leq C(\sigma_e^2, \Lambda_b) \sum_{x \in \mathcal{C}_R} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}.$$

Probability of Eve's Correct Decision

Given the above scheme to be employed by Alice, what is the probability that Eve correctly decodes the data c? It is known that this probability can be estimated by

$$P_e \leq C(\sigma_e^2, \Lambda_b) \sum_{x \in \mathcal{C}_R} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}. \tag{6}$$

This bound motivates the following design criteria for Eve's lattice. For a fixed dimension n, find the lattice Λ which minimizes the *inverse norm sum*

$$\boxed{S_\Lambda(R, s) = \sum_{x \in \mathcal{C}_R} \prod_{x_i \neq 0} \frac{1}{|x_i|^s}} \tag{7}$$

Algebraic Lattices

From now on, we'll only deal with the case of $n = 2$. For *algebraic lattices*, the inverse norm sum takes a particularly interesting form.

Let $K = \mathbf{Q}(\sqrt{d})$ be a totally real quadratic number field with ring of integers $\mathcal{O}_K$, and $\mathrm{Gal}(K/\mathbf{Q}) = \langle \sigma \rangle$.

For example, one could take $K = \mathbf{Q}(\sqrt{5})$, so that $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ and $\sigma(\sqrt{5}) = -\sqrt{5}$.

Algebraic Lattices

We can embed $\mathcal{O}_K \hookrightarrow \mathbf{R}^2$ as a lattice Λ via the *canonical embedding*

$$\Lambda := \{(x, \sigma(x)) : x \in \mathcal{O}_K\}. \tag{8}$$

In this case, the inverse norm sum becomes

$$S_\Lambda(R, s) = \sum_{x \in \mathcal{C}_R} \prod_{x_i \neq 0} \frac{1}{|x_i|^s} = \sum_{x \in \mathcal{C}_R} \frac{1}{|N(x)|^s} \tag{9}$$

where $N : K \to \mathbf{Q}$ is the *field norm*, defined by $N(x) = x \cdot \sigma(x)$.

The Inverse Norm Sum

From now on, we identify $\mathcal{O}_K$ with the lattice Λ it determines in $\mathbf{R}^2$. How do we estimate

$$S_\Lambda(R, s) = \sum_{\substack{x \in \mathcal{O}_K \\ ||x||_\infty \leq R}} \frac{1}{|N(x)|^s}, \tag{10}$$

and study how it grows as $R \to \infty$?

For any $x \in \mathcal{O}_K$, we have $N(x) \in \mathbf{Z}$. Thus any $x \in \mathcal{O}_K$ lives on one of the hyperbolas $XY = \pm k$ for some integer k, allowing for a convenient geometrical grouping of the codewords.

Estimating the Inverse Norm Sum

Now let

$$b_{k,R} = \#\{x \in \mathcal{O}_K : |N(x)| = k, ||x||_\infty \leq R\} \tag{11}$$

so that, for example, $b_{1,R}$ is the number of units inside the bounding box.

Estimating the Inverse Norm Sum

Now let

$$b_{k,R} = \#\{x \in \mathcal{O}_K : |N(x)| = k, ||x||_\infty \leq R\} \tag{11}$$

so that, for example, $b_{1,R}$ is the number of units inside the bounding box.

We have the following bounds for $S_\Lambda(R,s)$:

$$\boxed{b_{1,R} \leq S_\Lambda(R,s) \leq \zeta_K^1(s) b_{1,R}}, \tag{12}$$

where

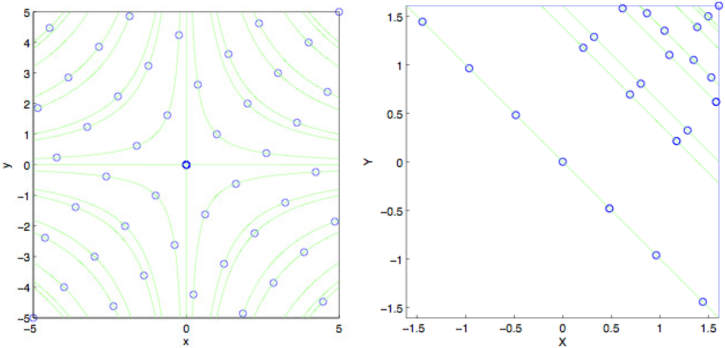
$$\zeta_K^1(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \mathfrak{a} \text{ principal}}} \frac{1}{N(\mathfrak{a})^s} = \sum_{k \geq 1} \frac{a_k^1}{k^s} \tag{13}$$

is the *partial zeta function* of K, so that a_k^1 is the number of principal ideals of norm k in $\mathcal{O}_K$.

Proof: (See also paper by Vehkalahti et al) Rewrite the inverse norm sum as

$$S_\Lambda(R,s) = \sum_{\substack{x \in \mathcal{O}_K \\ ||x||_\infty \leq R}} \frac{1}{|N(x)|^s} = \sum_{k \geq 1} \frac{b_{k,R}}{k^s}. \tag{14}$$

Taking $\log|\cdot|$ of each coordinate, one sees that $b_{k,R} \leq a_k^1 b_{1,R}$ for all $k > 0$:



Experimental Data

How good are these estimates? Let's take $K = \mathbf{Q}(\sqrt{5})$:

$\lfloor \log(R) \rfloor$	$b_{1,R}$	$S_\Lambda(R,3)$	$b_{1,R}\zeta_K^1(3)$
1	10	10.0472	10.2755
2	18	18.2576	18.4959
3	26	26.4809	26.7162
4	34	34.7068	34.9366
5	42	42.9276	43.1570
6	50	51.2105	51.3774

In order for these estimates to be practically useful, we have to have a way of calculating $\zeta_K^1(s)$, which is equivalent to calculating a_k^1 for $k = 1, \ldots, N$.

Evaluating the Partial Zeta Function

First, let us suppose that $k = p$ is prime, and we wish to calculate the number a_p^1 of principal ideals of norm p in $\mathcal{O}_K$.

The only ideals, principal or otherwise, in K which have norm p, must appear in the prime factorization of the ideal (p) in $\mathcal{O}_K$.

Evaluating the Partial Zeta Function

First, let us suppose that $k = p$ is prime, and we wish to calculate the number a_p^1 of principal ideals of norm p in $\mathcal{O}_K$.

The only ideals, principal or otherwise, in K which have norm p, must appear in the prime factorization of the ideal (p) in $\mathcal{O}_K$.

Let D be the discriminant of K. The ideal (p) factors in $\mathcal{O}_K$ as

$$(p) = \begin{cases} (p) \text{ is prime} & \text{iff } (p, D) = 1, D \not\equiv y^2 \pmod{p}, \text{ for any } y \in \mathbf{Z} \\ \mathfrak{p}\mathfrak{q}, \mathfrak{p} \neq \mathfrak{q} & \text{iff } (p, D) = 1, D \equiv y^2 \pmod{p}, \text{ for some } y \in \mathbf{Z} \\ \mathfrak{p}^2 & \text{iff } p \mid D \end{cases} \tag{15}$$

and we say that p is *inert*, *split*, or *ramified* in K, respectively.

Evaluating the Partial Zeta Function

If p is inert, so that (p) is prime, then the only prime ideal appearing in the factorization of (p) is (p) itself. But this ideal has norm p^2, so in this case $a_p^1 = 0$.

Evaluating the Partial Zeta Function

If p is inert, so that (p) is prime, then the only prime ideal appearing in the factorization of (p) is (p) itself. But this ideal has norm p^2, so in this case $a_p^1 = 0$.

If p is split, so that $(p) = \mathfrak{p}\mathfrak{q}$, then $\mathfrak{p}$ and $\mathfrak{q}$ are Galois conjugate and therefore simultaneously principal or non-prinicipal. Hence $a_p^1 = 0$ or 2, accordingly.

Evaluating the Partial Zeta Function

If p is inert, so that (p) is prime, then the only prime ideal appearing in the factorization of (p) is (p) itself. But this ideal has norm p^2, so in this case $a_p^1 = 0$.

If p is split, so that $(p) = \mathfrak{p}\mathfrak{q}$, then $\mathfrak{p}$ and $\mathfrak{q}$ are Galois conjugate and therefore simultaneously principal or non-prinicipal. Hence $a_p^1 = 0$ or 2, accordingly.

If p is ramified, so that $(p) = \mathfrak{p}^2$, then $\mathfrak{p}$ is the only ideal of norm p. So $a_p^1 = 0$ or 1, depending on whether $\mathfrak{p}$ is principal.

Algorithms for determining whether or not an ideal in a ring of integers is principal are implemented in SAGE.

Evaluating the Partial Zeta Function

What to do if $k = p_1^{e_1} \cdots p_m^{e_m}$ is not prime?

If k is composite, one can use the prime factorization of k, and how the p_i factor in K, to list all of the ideals of norm k. It's easier to see this by example.

Evaluating the Partial Zeta Function

Example: Let $K = \mathbf{Q}(\sqrt{229})$, and let $k = 225 = 3^2 \cdot 5^2$. Let us calculate a^1_{225}. In K the ideals (3) and (5) both split, and we have factorizations

$$\begin{aligned}(3) &= \mathfrak{p}_3\mathfrak{q}_3,\ \mathfrak{p}_3 = \left(3,\ (1-\sqrt{229})/2\right),\ \mathfrak{q}_3 = \left(3,\ (1+\sqrt{229})/2\right)\\ (5) &= \mathfrak{p}_5\mathfrak{q}_5,\ \mathfrak{p}_5 = \left(5,\ (7-\sqrt{229})/2\right),\ \mathfrak{q}_5 = \left(5,\ (7+\sqrt{229})/2\right)\end{aligned}$$

Evaluating the Partial Zeta Function

Example: Let $K = \mathbf{Q}(\sqrt{229})$, and let $k = 225 = 3^2 \cdot 5^2$. Let us calculate a^1_{225}. In K the ideals (3) and (5) both split, and we have factorizations

$$\begin{aligned}(3) &= \mathfrak{p}_3\mathfrak{q}_3,\ \mathfrak{p}_3 = \left(3,\ (1-\sqrt{229})/2\right),\ \mathfrak{q}_3 = \left(3,\ (1+\sqrt{229})/2\right)\\ (5) &= \mathfrak{p}_5\mathfrak{q}_5,\ \mathfrak{p}_5 = \left(5,\ (7-\sqrt{229})/2\right),\ \mathfrak{q}_5 = \left(5,\ (7+\sqrt{229})/2\right)\end{aligned}$$

thus the list of all ideals of norm k is

$$\mathfrak{p}_3^2\mathfrak{p}_5^2,\ \mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5^2,\ \mathfrak{q}_3^2\mathfrak{p}_5^2,\ \mathfrak{p}_3^2\mathfrak{p}_5\mathfrak{q}_5,\ \mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5\mathfrak{q}_5,\ \mathfrak{q}_3^2\mathfrak{p}_5\mathfrak{q}_5,\ \mathfrak{p}_3^2\mathfrak{q}_5^2,\ \mathfrak{p}_3\mathfrak{q}_3\mathfrak{q}_5^2,\ \mathfrak{q}_3^2\mathfrak{q}_5^2.$$

Exactly three of these ideals are principal, so that $a^1_{225} = 3$. Specifically,

$$\mathfrak{p}_3^2\mathfrak{q}_5^2 = (2-\sqrt{229}),\ \mathfrak{p}_3\mathfrak{q}_3\mathfrak{q}_5^2 = (2+\sqrt{229}),\ \mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5\mathfrak{q}_5 = (15).$$

Conclusion

Design criteria for coset coding using algebraic lattices over fading wiretap channels consists of studying the inverse norm sum,

$$S_\Lambda(R, s) = \sum_{\substack{x \in \mathcal{O}_K \\ ||x||_\infty \leq R}} \frac{1}{|N(x)|^s}, \tag{16}$$

which itself is inversely proportional to the regulator of K, and directly proportional to the values of the partial zeta function of K.

Further work consists of studying for which number fields both of these quantities are optimal, as well as extending results to MIMO systems.

The End! Thanks!

The End! Thanks!

References

1. F. Oggier, J.C. Belfiore, and E. Viterbo, *Cyclic Division Algebras: A Tool for Space-Time Coding*, Foundations and Trends in Communications and Information Theory. 2007. Vol. 4, No 1, pp 1-95.

2. J.C. Belfiore and F. Oggier, *An Error Probability Approach to MIMO Wiretap Channels*, January 2013, `http://arxiv.org/abs/1109.6437`.

3. R. Vehkalahti, F. Lu, and L. Luzzi, *Inverse Determinant Sums and Connections Between Fading Channel Information Theory and Algebra*, December 2012, `http://arxiv.org/abs/1111.6289`.

4. C. Hollanti, E. Viterbo, and D. Karpuk, *Nonasymptotic Probability Bounds for Fading Channels Exploiting Dedekind Zeta Functions*, January 2013, `http://arxiv.org/abs/1303.3475`.