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

\[ y_b = H_b x + z_b \]  \hspace{1cm} (1)  
\[ y_e = H_e x + z_e \]  \hspace{1cm} (2)  

where

- \( x \in \mathbb{R}^n \) is the vector intended for transmission.

- \( H_b, H_e \in \mathbb{M}_{n \times n}(\mathbb{R}) \) are Bob's and Eve's fading matrices, respectively.

- \( z_b, z_e \in \mathbb{R}^n \) are the corresponding noise vectors, whose entries are Gaussian random variables with variance \( \sigma_b^2, \sigma_e^2 \).

- \( y_b, y_e \in \mathbb{R}^n \) are the vectors received by Bob and Eve.

We assume that \( \sigma_e^2 \gg \sigma_b^2 \), i.e. that Eve's channel is much noisier than Bob's.
This wireless channel can be modeled by the equations

\[ y_b = H_b x + z_b \]  \hspace{1cm} (1) \\
\[ y_e = H_e x + z_e \]  \hspace{1cm} (2)

where

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

\[ \sigma^2_e \gg \sigma^2_b \]
This wireless channel can be modeled by the equations

\begin{align*}
y_b &= H_b x + z_b \\
y_e &= H_e x + z_e
\end{align*}

where

- \( x \in \mathbb{R}^n \) is the vector intended for transmission.
- \( H_b, H_e \in M_n(\mathbb{R}) \) are Bob’s and Eve’s fading matrices, respectively.
- \( z_b, z_e \in \mathbb{R}^n \) are the corresponding noise vectors, whose entries are Gaussian random variables with variance \( \sigma_b^2, \sigma_e^2 \).
This wireless channel can be modeled by the equations

\[ y_b = H_b x + z_b \]  \hspace{1cm} (1) \\
\[ y_e = H_e x + z_e \]  \hspace{1cm} (2)

where

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

This wireless channel can be modeled by the equations

\[ y_b = H_b x + z_b \]  
\[ y_e = H_e x + z_e \]

where

- \( x \in \mathbb{R}^n \) is the vector intended for transmission.
- \( H_b, H_e \in M_n(\mathbb{R}) \) are Bob’s and Eve’s fading matrices, respectively.
- \( z_b, z_e \in \mathbb{R}^n \) are the corresponding noise vectors, whose entries are Gaussian random variables with variance \( \sigma_b^2, \sigma_e^2 \).
- \( y_b, y_e \in \mathbb{R}^n \) 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.
Alice uses *coset coding*, a variant of lattice coding, to confuse Eve.

Alice selects a “fine” lattice $\Lambda_b$ whose elements encode data intended for Bob. At the same time, Alice chooses a “coarse” sublattice

$$\Lambda_e \subset \Lambda_b,$$

containing random bits intended to confuse Eve.
Alice now sends codewords of the form

\[ x = r + c \]  \hspace{1cm} (4)

where \( r \) is a random element of \( \Lambda_e \) intended to confuse Eve, and \( c \) is a coset representative of \( \Lambda_e \) in \( \Lambda_b \).

Alice’s strategy ensures that Eve can easily recover the “random” data \( r \), but not the actual data \( c \).
In practice, we construct Eve’s codebook from a finite subset $C_R$ of $\Lambda_e$, which we’ll define as

$$C_R := \{x \in \Lambda_e : \|x\|_{\infty} \leq R\}$$

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

![Diagram with blue dots and lines]

David Karpuk (Aalto University)

Probability Bounds for Two-Dimensional April 16, 2013 6 / 20
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

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

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

This bound motivates the following design criteria for Eve’s lattice. For a fixed dimension $n$, find the lattice $\Lambda$ which minimizes the inverse norm sum

$$S_{\Lambda}(R, s) = \sum_{x \in \mathcal{C}_R} \prod_{x_i \neq 0} \frac{1}{|x_i|^s}. \quad (7)$$
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 \( K = \mathbb{Q}(\sqrt{d}) \) be a totally real quadratic number field with ring of integers \( \mathcal{O}_K \), and \( \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle \).

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

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

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

In this case, the inverse norm sum becomes

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

where $N : K \rightarrow \mathbb{Q}$ 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 $\Lambda$ it determines in $\mathbb{R}^2$. How do we estimate

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

(10)

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

For any $x \in \mathcal{O}_K$, we have $N(x) \in \mathbb{Z}$. 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

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

so that, for example, \( b_{1,R} \) is the number of units inside the bounding box.
Estimating the Inverse Norm Sum

Now let

\[ b_{k,R} = \#\{x \in \mathcal{O}_K : |N(x)| = k, ||x||_\infty \leq R\} \]  \hspace{1cm} (11)

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

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

\[ b_{1,R} \leq S_\Lambda(R, s) \leq \zeta_1^K(s)b_{1,R}, \] \hspace{1cm} (12)

where

\[ \zeta_1^K(s) = \sum_{a \subseteq \mathcal{O}_K \text{ principal}} \frac{1}{N(a)^s} = \sum_{k \geq 1} \frac{a_k^1}{k^s} \]  \hspace{1cm} (13)

is the partial zeta function of \( K \), so that \( a_k^1 \) is the number of principal ideals of norm \( k \) in \( \mathcal{O}_K \).
Estimating the Inverse Norm Sum

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

\[ S_\Lambda(R, s) = \sum_{x \in \mathcal{O}_K} \frac{1}{|N(x)|^s} = \sum_{k \geq 1} \frac{b_{k,R}}{k^s}. \]  

(14)

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

![Graphs showing the inverse norm sum and its components](image-url)
How good are these estimates? Let’s take $K = Q(\sqrt{5})$:

<table>
<thead>
<tr>
<th>$\lfloor \log(R) \rfloor$</th>
<th>$b_{1,R}$</th>
<th>$S_\Lambda(R, 3)$</th>
<th>$b_{1,R}\zeta_1^1(K)(3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>10.0472</td>
<td>10.2755</td>
</tr>
<tr>
<td>2</td>
<td>18</td>
<td>18.2576</td>
<td>18.4959</td>
</tr>
<tr>
<td>3</td>
<td>26</td>
<td>26.4809</td>
<td>26.7162</td>
</tr>
<tr>
<td>4</td>
<td>34</td>
<td>34.7068</td>
<td>34.9366</td>
</tr>
<tr>
<td>5</td>
<td>42</td>
<td>42.9276</td>
<td>43.1570</td>
</tr>
<tr>
<td>6</td>
<td>50</td>
<td>51.2105</td>
<td>51.3774</td>
</tr>
</tbody>
</table>

In order for these estimates to be practically useful, we have to have a way of calculating $\zeta_1^1(K)(s)$, 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

\[
(p) = \begin{cases} 
(p) \text{ is prime} & \text{iff } (p, D) = 1, D \not\equiv y^2 \pmod{p}, \text{ for any } y \in \mathbb{Z} \\
pq, p \neq q & \text{iff } (p, D) = 1, D \equiv y^2 \pmod{p}, \text{ for some } y \in \mathbb{Z} \\
p^2 & \text{iff } p | D 
\end{cases}
\]

(15)

and we say that \( p \) is inert, split, or ramified in \( K \), respectively.
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 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 $(p) = pq$, then $p$ and $q$ are Galois conjugate and therefore simultaneously principal or non-principal. 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 \((p) = pq\), then \( p \) and \( q \) are Galois conjugate and therefore simultaneously principal or non-principal. Hence \( a_p^1 = 0 \) or \( 2 \), accordingly.

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

Algorithms for determining whether or not an ideal in a ring of integers is principal are implemented in SAGE.
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.
Example: Let $K = \mathbb{Q}(\sqrt{229})$, and let $k = 225 = 3^2 \cdot 5^2$. Let us calculate $a_{225}$. In $K$ the ideals (3) and (5) both split, and we have factorizations

\begin{align*}
(3) &= p_3q_3, \quad p_3 = \left(3, \frac{1 - \sqrt{229}}{2}\right), \quad q_3 = \left(3, \frac{1 + \sqrt{229}}{2}\right) \\
(5) &= p_5q_5, \quad p_5 = \left(5, \frac{7 - \sqrt{229}}{2}\right), \quad q_5 = \left(5, \frac{7 + \sqrt{229}}{2}\right)
\end{align*}
Evaluating the Partial Zeta Function

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

$$(3) = p_3q_3, \quad p_3 = \left(3, (1 - \sqrt{229})/2\right), \quad q_3 = \left(3, (1 + \sqrt{229})/2\right)$$

$$(5) = p_5q_5, \quad p_5 = \left(5, (7 - \sqrt{229})/2\right), \quad q_5 = \left(5, (7 + \sqrt{229})/2\right)$$

thus the list of all ideals of norm $k$ is

$p_3^2p_5^2, \ p_3q_3p_5^2, \ q_3^2p_5^2, \ p_3^2p_5q_5, \ p_3q_3p_5q_5, \ q_3^2p_5q_5, \ p_3q_5^2, \ p_3q_3q_5^2, \ q_3q_5^2$.

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

$p_3^2q_5^2 = (2 - \sqrt{229}), \ p_3q_3q_5^2 = (2 + \sqrt{229}), \ p_3q_3p_5q_5 = (15)$. 
Conclusion

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

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

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!
References


