Lattice Network Coding over Finite Rings

Chen Feng
Department of Electrical & Computer Engineering
University of Toronto, Canada

joint work with:
Danilo Silva, Federal University of Santa Catarina, Brazil, and
Frank R. Kschischang, University of Toronto

CWIT 2011, Kelowna, British Columbia, Canada
19 May, 2011
Background: Physical-Layer Network Coding


Key idea: decode $w_1 \oplus w_2$ and then broadcast
More elaborate schemes approach the cut-set bound for two-way relay channels e.g., Narayanan-Wilson-Sprintson 2007, Nam-Chung-Lee 2008
Background: Physical-Layer Network Coding
Background: Physical-Layer Network Coding
Background: Physical-Layer Network Coding

\[ y_3 = h_{13}x_1 + h_{23}x_2 + z_3 \]

\[ y_4 = h_{14}x_1 + h_{24}x_2 + z_4 \]
Background: Physical-Layer Network Coding

\[ w_3 = a_{13}w_1 + a_{23}w_2 \]
\[ y_3 = h_{13}x_1 + h_{23}x_2 + z_3 \]
\[ w_4 = a_{14}w_1 + a_{24}w_2 \]
\[ y_4 = h_{14}x_1 + h_{24}x_2 + z_4 \]
Background: Physical-Layer Network Coding

\[ w_3 = a_{13} w_1 + a_{23} w_2 \]

\[ w_4 = a_{14} w_1 + a_{24} w_2 \]
Background: Physical-Layer Network Coding

\[ w_3 = a_{13} w_1 + a_{23} w_2 \]

\[ w_4 = a_{14} w_1 + a_{24} w_2 \]

\[ y_5 = h_{35} x_3 + h_{45} x_4 + z_5 \]
Background: Physical-Layer Network Coding

\[ w_1 \]

\[ w_2 \]

\[ w_3 = a_{13} w_1 + a_{23} w_2 \]

\[ w_3 \]

\[ w_4 = a_{14} w_1 + a_{24} w_2 \]

\[ w_4 \]

\[ w_5 = a_{35} w_3 + a_{45} w_4 \]

\[ w_5 \]

\[ y_5 = h_{35} x_3 + h_{45} x_4 + z_5 \]
Abstraction: Computation over a Gaussian MAC

\[ \mathbf{w}_1 \in \mathbb{F}_q^k \rightarrow \mathcal{E} \rightarrow \mathbf{x}_1 \in \mathbb{C}^n \]
\[ \mathbf{w}_2 \in \mathbb{F}_q^k \rightarrow \mathcal{E} \rightarrow \mathbf{x}_2 \in \mathbb{C}^n \]
\[ \vdots \]
\[ \mathbf{w}_L \in \mathbb{F}_q^k \rightarrow \mathcal{E} \rightarrow \mathbf{x}_L \in \mathbb{C}^n \]
\[ \mathbf{u} = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell \]
\[ \mathbf{y} = \sum_{\ell=1}^{L} h_\ell \mathbf{x}_\ell + z \]

**Setup**

Message rate: \( R_{\text{mes}} \triangleq k \log_2(q)/n \);

Probability of error: \( P_e \triangleq \Pr[\hat{u} \neq u] \)

**Objective**

maximize \( R_{\text{mes}} \) subject to power constraint and error constraint
Nazer-Gastpar’s Approach

A lattice-partition-based approach (Nazer-Gastpar 2008)

Bird’s eye view: transmitters — the same lattice partition
receiver — three simple components
Nazer-Gastpar’s Approach

A lattice-partition-based approach (Nazer-Gastpar 2008)

Bird’s eye view: transmitters — the same lattice partition
receiver — three simple components

Main result: \( R_{\text{mes}} = \log_2 \left( \frac{\text{SNR}}{(|\alpha|^2 + \text{SNR} \sum_{\ell} |\alpha h_\ell - a_\ell|^2)} \right) \)

Assumption: lattice partitions proposed by Erez and Zamir (2004)
Problem Considered in This Work

Note that...

Erez-Zamir’s construction is similar to Shannon’s random-code construction

What if practical lattice partitions are used?

- efficient encoding and decoding
- finite (or short) packet length
A Toy Example (integer-valued case)

Each transmitter applies the same lattice partition $\Lambda/\Lambda'$
A Toy Example (integer-valued case)

Transmitter 1 maps $w_1$ to a constellation point
A Toy Example (integer-valued case)

Transmitter 2 maps $\mathbf{w}_2$ to a constellation point
A Toy Example (integer-valued case)

The channel is given by \( y = 2x_1 + x_2 + z \)
A Toy Example (integer-valued case)

\[ y = h_1 x_1 + h_2 x_2 + z \]

\[ (h_1, h_2) = (2, 1) \]

Hence, the received signal \( y \) is like this
A Toy Example (integer-valued case)

\[ y = h_1 x_1 + h_2 x_2 + z \]

\( (h_1, h_2) = (2, 1) \)

But how can we extract some information from \( y \)?
A Toy Example (integer-valued case)

\[ y = h_1 x_1 + h_2 x_2 + z \]

\[ (h_1, h_2) = (2, 1) \]

The receiver can decode \(2x_1 + x_2\)
A Toy Example (integer-valued case)

Note that...

one can construct a one-to-one linear map between $\mathbb{F}_3^2$ and $\Lambda/\Lambda'$

$w_1 = (1, 0)$

$w_2 = (0, 1)$

$\hat{u} = (2, 1)$

$\hat{u} = 2w_1 + w_2$

Hence, an integer combination of lattice points

$= \text{a linear combination of messages}$
What if the channel gains are real numbers or complex numbers?

Answer:

\[ \alpha y = \sum_{\ell=1}^{L} \alpha h_\ell x_\ell + \alpha z \]

Remark: see [CISS 2011] for details.
What if the channel gains are real numbers or complex numbers?

**Answer:** apply a scaling operation

\[ \alpha y = \sum_{\ell} \alpha h_{\ell} x_{\ell} + \alpha z \]

\[ = \sum_{\ell} \left\lfloor \alpha h_{\ell} \right\rfloor x_{\ell} + \sum_{\ell} (\alpha h_{\ell} - \left\lfloor \alpha h_{\ell} \right\rfloor) x_{\ell} + \alpha z \]

- effective noise

Remark: see [CISS 2011] for details
What if the channel gains are real numbers or complex numbers?

**Answer:** apply a scaling operation

\[ \alpha y = \sum_{\ell} \alpha h_\ell x_\ell + \alpha z \]

\[ \begin{align*}
&= \sum_{\ell} \lfloor \alpha h_\ell \rfloor x_\ell + \sum_{\ell} (\alpha h_\ell - \lfloor \alpha h_\ell \rfloor) x_\ell + \alpha z \\
&\quad \underbrace{\text{effective noise}}
\end{align*} \]

**Remark:** see [CISS 2011] for details
A Short Summary So Far

When a practical lattice partition is used...

1. one shall choose a “good” scalar $\alpha$ [CISS 2011]
2. one shall decode a lattice point
3. one shall construct a **one-to-one linear map**
Let $C$ be the [16, 15, 2] even weight code.

Construct a lattice $D_{16} = 2\mathbb{Z}^{16} + C$.

$D_{16}$ is called a checkboard lattice.

This procedure is called Construction A.
Construct Linear Maps: Example 1

**Checkboard lattice**

Let $C$ be the $[16, 15, 2]$ even weight code.

Construct a lattice $D_{16} = 2\mathbb{Z}^{16} + C$.

$D_{16}$ is called a checkboard lattice.

This procedure is called **Construction A**.

**A natural lattice partition**

$D_{16}/2\mathbb{Z}^{16}$ is a lattice partition with $2^{15}$ cosets.

Each coset corresponds to a codeword in $C$. 
Construct Linear Maps: Example 1

**Checkboard lattice**

Let $C$ be the $[16, 15, 2]$ even weight code.

Construct a lattice $D_{16} = 2\mathbb{Z}^{16} + C$.

$D_{16}$ is called a checkboard lattice.

This procedure is called **Construction A**.

**A natural lattice partition**

$D_{16}/2\mathbb{Z}^{16}$ is a lattice partition with $2^{15}$ cosets.

Each coset corresponds to a codeword in $C$.

**A one-to-one linear map** can be constructed as

$2\mathbb{Z}^{16} + uG_C \rightarrow u$
Barnes-Wall lattice

Let $C^{(1)}$ be the $[16, 15, 2]$ even weight code.

Let $C^{(2)}$ be the $[16, 5, 8]$ Reed-Muller code.

Construct a lattice $\Lambda_{16} = 4\mathbb{Z}^{16} + 2C^{(1)} + C^{(2)}$.

$\Lambda_{16}$ is called a Barnes-Wall lattice.

This procedure is called Construction D.
Barnes-Wall lattice

Let \( C^{(1)} \) be the \([16, 15, 2]\) even weight code.
Let \( C^{(2)} \) be the \([16, 5, 8]\) Reed-Muller code.
Construct a lattice \( \Lambda_{16} = 4\mathbb{Z}^{16} + 2C^{(1)} + C^{(2)} \).
\( \Lambda_{16} \) is called a Barnes-Wall lattice.
This procedure is called Construction D.

A natural lattice partition

\( \Lambda_{16}/4\mathbb{Z}^{16} \) is a lattice partition with \( 2^{15+5} \) cosets.
Each coset corresponds to two codewords \((c^{(1)}, c^{(2)})\).
Let $C^{(1)}$ be the [16, 15, 2] even weight code.
Let $C^{(2)}$ be the [16, 5, 8] Reed-Muller code.
Construct a lattice $\Lambda_{16} = 4\mathbb{Z}^{16} + 2C^{(1)} + C^{(2)}$.
$\Lambda_{16}$ is called a Barnes-Wall lattice.
This procedure is called Construction D.

$\Lambda_{16}/4\mathbb{Z}^{16}$ is a lattice partition with $2^{(15+5)}$ cosets.
Each coset corresponds to two codewords $(c^{(1)}, c^{(2)})$.

A map can be constructed as
$$4\mathbb{Z}^{16} + 2u^{(1)} G_{C^{(1)}} + u^{(2)} G_{C^{(2)}} \rightarrow (u^{(1)}, u^{(2)})$$
Warning!

\[ 4\mathbb{Z}^{16} + 2u^{(1)} G_{C(1)} + u^{(2)} G_{C(2)} \rightarrow (u^{(1)}, u^{(2)}) \]

This map is **one-to-one**, but not **linear**
Warning!

$$4\mathbb{Z}^{16} + 2u^{(1)}G_{C(1)} + u^{(2)}G_{C(2)} \rightarrow (u^{(1)}, u^{(2)})$$

This map is one-to-one, but not linear

Why?

Consider

$$4\mathbb{Z}^{16} + [1, \ldots, 1]G_{C(2)} \rightarrow (0, \ldots, 0, 1, \ldots, 1)$$

If the map is linear, then...

$$4\mathbb{Z}^{16} + [2, \ldots, 2]G_{C(2)} \rightarrow (0, \ldots, 0, 0, \ldots, 0)$$

This implies...

$$[2, \ldots, 2]G_{C(2)} \in 4\mathbb{Z}^{16}$$
Construct a one-to-one linear map for Example 2

Key idea: codes over integer residue rings [Blake 1975]
Construct Linear Maps: A Bit More Algebra

Construct a one-to-one linear map for Example 2
Key idea: codes over integer residue rings [Blake 1975]

Construct a one-to-one linear map in general
Key idea: Smith normal form of a matrix over PIDs
Construct a one-to-one linear map for Example 2
Key idea: codes over integer residue rings [Blake 1975]

Construct a one-to-one linear map in general
Key idea: Smith normal form of a matrix over PIDs

Theorem
Let $\Lambda/\Lambda'$ be a lattice partition. Then there exist generator matrices $G_\Lambda$ and $G_{\Lambda'}$ satisfying

$$G_{\Lambda'} = \begin{bmatrix} \text{diag}(\pi_1, \ldots, \pi_k) & 0 \\ 0 & I_{N-k} \end{bmatrix} G_\Lambda,$$

where $\pi_1 | \pi_2 | \cdots | \pi_k$.

The map $\varphi(rG_\Lambda) = (r_1 + (\pi_1), \ldots, r_k + (\pi_k))$ is indeed one-to-one and linear.
What does it buy us?

Recall that

\[ D_{16} = 2\mathbb{Z}^{16} + C^{(1)} \text{ or } 2D_{16} = 4\mathbb{Z}^{16} + 2C^{(1)} \]
\[ \Lambda_{16} = 4\mathbb{Z}^{16} + 2C^{(1)} + C^{(2)} \]

Compare

\[ 2D_{16}/4\mathbb{Z}^{16} \ (2^{15} \text{ cosets}) \text{ and } \Lambda_{16}/4\mathbb{Z}^{16} \ (2^{20} \text{ cosets}) \]

Note that

their minimum Euclidean distances are the same

This implies

same error performance with higher message rate
Related Work

**Related work on performance analysis**
- Feng-Silva-Kschischang (2011)

**Related work on construction of lattice partitions**
- Based on LDPC codes
  - Ordentlich-Erez (2010)
- Based on multilevel coding
  - Hern-Narayanan (2010)
- Based on signal codes
  - Feng-Silva-Kschischang (2010)
Conclusions

1. **How to use practical lattice partitions**
   - choose a good scalar $\alpha$
   - decode a lattice point
   - construct a one-to-one linear map

2. **How to construct linear maps**
   - Construct A: simple
   - Construct D: linear codes over rings
   - General: Smith normal form
Thank You!
Backup Slides