An Introduction to Physical Layer Network Coding: Lattice Codes as Groups

Brian M. Kurkoski
Japan Advanced Institute of Science and Technology

September 11, 2015
Sendai, Miyagi, Japan
Cooperative Wireless Networks

Wireless networks must deal with interference & noise
Overview

1 Motivation for physical-layer network coding
   1A Network Coding
   1B Physical Layer Network Coding

2 Nested Lattice Codes
   2A Quotient Groups
   2B Lattice Quotient Groups
   2C Nested Lattice Codes

3 Encoding and Isomorphisms in Nested Lattice Codes
   3A Self-similar Voronoi codes
   3B Non-Self-similar Voronoi Codes
Routing vs. Network Coding

Capacity: max rate from source to destination

Routing

- Capacity = $3/2$
Routing vs. Network Coding

Capacity: max rate from source to destination

Routing
- Capacity = $3/2$

Network Coding
- Internal nodes perform linear operations
- Capacity = 2

Forwarding combinations of messages can increase capacity
Matrix Form Recovery of Messages

2 received messages and 2 desired messages:

\[
\begin{bmatrix}
  u_1 \\
  u_2
\end{bmatrix} = \begin{bmatrix}
  1 & 0 \\
  1 & 1
\end{bmatrix} \cdot \begin{bmatrix}
  w_1 \\
  w_2
\end{bmatrix}
\]

\[
\begin{bmatrix}
  1 & 0 \\
  1 & 1
\end{bmatrix}^{-1} \cdot \begin{bmatrix}
  u_1 \\
  u_2
\end{bmatrix} = \begin{bmatrix}
  w_1 \\
  w_2
\end{bmatrix}
\]

received messages  
\[\uparrow\]  
desired messages
$w, u, q$ in a field. Allow relay to multiply by $q$

$$Q = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1L} \\ q_{21} & q_{22} & \cdots & q_{2L} \\ & & \ddots & \vdots \\ q_{M1} & q_{M2} & \cdots & q_{ML} \end{bmatrix}$$

If $Q$ has rank $L$, then all messages $w$ recoverable

How to design $Q$?

- Algorithmic approach (Jaggi et al.)
  - Success if field size $p >$ number of destinations
- Random approach (Kotter and Medard. Ho et al.)
  - Probability of valid solutions increases with $p$
Action of One Row
A “Relay”

Source has $w_1, w_2, \ldots$

Destination has $u_1, u_2, \ldots$

\[
\begin{bmatrix}
  u_1 \\
  u_2 \\
  \vdots \\
  u_M
\end{bmatrix}
= 
\begin{bmatrix}
  q_{11} & q_{12} & \cdots & q_{1L} \\
  q_{21} & q_{22} & \cdots & q_{2L} \\
  \vdots & \vdots & \ddots & \vdots \\
  q_{M1} & q_{M2} & \cdots & q_{ML}
\end{bmatrix}
\begin{bmatrix}
  w_1 \\
  w_2 \\
  \vdots \\
  w_L
\end{bmatrix}
\]

received messages
desired messages
Action of One Row
A “Relay”

\[
\begin{bmatrix}
    u_1 \\
    u_2 \\
    \vdots \\
    u_M
\end{bmatrix}
= 
\begin{bmatrix}
    q_{11} & q_{12} & \cdots & q_{1L} \\
    q_{21} & q_{22} & \cdots & q_{2L} \\
    \vdots & \vdots & \ddots & \vdots \\
    q_{M1} & q_{M2} & \cdots & q_{ML}
\end{bmatrix}
\begin{bmatrix}
    w_1 \\
    w_2 \\
    \vdots \\
    w_L
\end{bmatrix}
\]

received messages

desired messages

What if the relay is wireless...?
PLNC = Physical Layer Network Coding

$y = x_1 + \ldots + x_M + \text{noise}$

Addition occurs over the air

Wireless Multiple-Access Channel
**Network Coding vs. PLNC**

**Network Coding:**
- Relay adds incoming messages.
- $q_1 w_1 \oplus q_2 w_2$

**Physical Layer Network Coding**
- $h_1 x_1 + h_2 x_2$
- Combats noise.

**PLNC:**
- Addition over the air.
- Fading plays a role.
Perform error-correction coding on vectors:

$$x_i = Enc(w_i)$$

Relay performs two functions:

$$x_1 + x_2 = Decoder(y)$$

$$w_1 \oplus w_2 = Enc^{-1}(x_1 + x_2)$$
Powerful idea:

- Relay only eliminates noise
- Relay does not need to separate inference
- Converted a noisy network into a noiseless network
We Need A Code to Perform PLNC

Code must correct errors, for noisy wireless channels
  • Code must satisfy a power constraint.

Code must form a group over addition
  • so addition over the channel makes sense.

Code must have a group isomorphism: \( \text{Enc}(\mathbf{w}_1 \oplus \mathbf{w}_2) = \mathbf{x}_1 + \mathbf{x}_2, \)
  • so network coding can be performed

These properties are satisfied by nested lattice codes.
Quotient Groups

\[ \frac{G}{H} \]

\[ \Lambda_c / \Lambda_s \]
Definition of a Coset

Definition Let \( G \) be a group and let \( H \) be a subgroup of \( G \). For any \( a \in G \), the set \( a + H = \{a + h \mid h \in H\} \) is called the coset of \( H \) in \( G \) containing \( a \).

Quotient Groups

Let \( G/H \) be the set of all cosets of \( H \) in \( G \), that is:

\[
G/H = \{a + H \mid a \in G\}
\]

Note that \( G/H \) is a set of sets. The set \( G/H \) is called a quotient group.
Example

- Integers $\mathbb{Z}$ are a group under addition.
- $4\mathbb{Z}$ is a subgroup: $4\mathbb{Z} \subset \mathbb{Z}$.
- The quotient group $\mathbb{Z}/4\mathbb{Z}$, has four sets:
  
  $0 + 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
  
  $1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
  
  $2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
  
  $3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

The quotient group is closed under addition:

<table>
<thead>
<tr>
<th></th>
<th>$0 + 4\mathbb{Z}$</th>
<th>$1 + 4\mathbb{Z}$</th>
<th>$2 + 4\mathbb{Z}$</th>
<th>$3 + 4\mathbb{Z}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 + 4\mathbb{Z}$</td>
<td>$0 + 4\mathbb{Z}$</td>
<td>$1 + 4\mathbb{Z}$</td>
<td>$2 + 4\mathbb{Z}$</td>
<td>$3 + 4\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 + 4\mathbb{Z}$</td>
<td>$1 + 4\mathbb{Z}$</td>
<td>$2 + 4\mathbb{Z}$</td>
<td>$3 + 4\mathbb{Z}$</td>
<td>$0 + 4\mathbb{Z}$</td>
</tr>
<tr>
<td>$2 + 4\mathbb{Z}$</td>
<td>$2 + 4\mathbb{Z}$</td>
<td>$3 + 4\mathbb{Z}$</td>
<td>$0 + 4\mathbb{Z}$</td>
<td>$1 + 4\mathbb{Z}$</td>
</tr>
<tr>
<td>$3 + 4\mathbb{Z}$</td>
<td>$3 + 4\mathbb{Z}$</td>
<td>$0 + 4\mathbb{Z}$</td>
<td>$1 + 4\mathbb{Z}$</td>
<td>$2 + 4\mathbb{Z}$</td>
</tr>
</tbody>
</table>
Coset Leader (Coset Representative)

A coset leader is a single representative element from each coset.

Continue $\mathbb{Z}/4\mathbb{Z}$ example:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>-2</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-2</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>-2</td>
<td>-2</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-2</td>
</tr>
</tbody>
</table>
A lattice $\Lambda$ is a linear additive subgroup of $\mathbb{R}^n$. $\Lambda$ may be represented by a basis of $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$. A lattice point $\mathbf{x} \in \Lambda$ is an integral, linear combination of the basis vectors:

$$\mathbf{x} = \mathbf{g}_1 b_1 + \mathbf{g}_2 b_2 + \cdots + \mathbf{g}_n b_n,$$

where the $b_i$ are integers.
Let $\Lambda_c$ be a lattice

- “coding lattice” corrects errors. Also called fine lattice.

Let $\Lambda_s$ be a sublattice: $\Lambda_s \subset \Lambda_c$.

- “shaping lattice” enforces power constraint. Also called coarse lattice.

$K\Lambda_c$ is a lattice expanded by $K$.

- Choosing $\Lambda_s = K\Lambda_c$ results in $\Lambda_s \subseteq \Lambda_c$ for $K = 1, 2, 3, \cdots$
Lattice (group) $\Lambda_c = A_2$
Sublattice (subgroup)
\[ \Lambda_s = 2A_2 \]
Sublattice condition:
\[ \Lambda_s \subseteq \Lambda_c \]
4 cosets. Coset containing $c_0, c_1, c_2, c_3$. 

\[ c_1 + \Lambda_s \]
\[ c_2 + \Lambda_s \]
\[ c_0 + \Lambda_s \]
\[ c_3 + \Lambda_s \]
Cosets form a group under addition

The set $\Lambda_c/\Lambda_s$ is a quotient group.

This table expresses group addition:

<table>
<thead>
<tr>
<th></th>
<th>$c_0 + \Lambda_s$</th>
<th>$c_1 + \Lambda_s$</th>
<th>$c_2 + \Lambda_s$</th>
<th>$c_3 + \Lambda_s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c_0 + \Lambda_s$</td>
<td>$c_0 + \Lambda_s$</td>
<td>$c_1 + \Lambda_s$</td>
<td>$c_2 + \Lambda_s$</td>
<td>$c_3 + \Lambda_s$</td>
</tr>
<tr>
<td>$c_1 + \Lambda_s$</td>
<td>$c_1 + \Lambda_s$</td>
<td>$c_0 + \Lambda_s$</td>
<td>$c_3 + \Lambda_s$</td>
<td>$c_2 + \Lambda_s$</td>
</tr>
<tr>
<td>$c_2 + \Lambda_s$</td>
<td>$c_2 + \Lambda_s$</td>
<td>$c_3 + \Lambda_s$</td>
<td>$c_0 + \Lambda_s$</td>
<td>$c_1 + \Lambda_s$</td>
</tr>
<tr>
<td>$c_3 + \Lambda_s$</td>
<td>$c_3 + \Lambda_s$</td>
<td>$c_2 + \Lambda_s$</td>
<td>$c_1 + \Lambda_s$</td>
<td>$c_0 + \Lambda_s$</td>
</tr>
</tbody>
</table>
Construct a lattice code $\mathcal{C}$:

$$\mathcal{C} = \Lambda_c \cap \mathcal{F}$$

We need:

- Quotient Group $\Lambda_c / \Lambda_s$
- $\mathcal{F}$ is a fundamental region for $\Lambda_s$

The code $\mathcal{C}$ are coset leaders $\Lambda_c / \Lambda_s$, and is a group.
A fundamental region $\mathcal{F} \subset \mathbb{R}^n$ is a shape that, if shifted by each lattice point, will exactly cover the whole real real space. Volume $V(\mathcal{F})$ of $\mathcal{F}$ is constant and $V(\mathcal{F}) = |\det \Lambda|$.
Selecting the Coset Leaders

\[ \mathcal{C} = \Lambda_c \cap \mathcal{F} \]
Nested Lattice Codes Form a Group

\[ \mathcal{C} = \Lambda_c \cap \mathcal{F} \]

codebook \( \mathcal{C} = \{c_0, c_1, c_2, c_3\} \)

\( c_i \) are coset leaders of \( \Lambda_c/\Lambda_s \).

\( \mathcal{C} \) is closed under addition.
Various Nested Lattice Codes

$\mathcal{F}$ defines the coset leaders:

3 Different Voronoi regions — All codes form Groups
Various Nested Lattice Codes

parallelotope
Important for theory, not very practical

Voronoi region
Best transmit power, not always easy to implement

(hyper-) rectangle
Rectangle
Easier to implement, no shaping gain
Voronoi is Best for AWGN Channel

Voronoi regions are sphere-like in high dimension.
A sphere satisfies the AWGN power constraint

\[
\frac{1}{n} \sum_{i=1}^{n} x_i^2 \leq P
\]
Encoding and Isomorphism

Encoding: mapping information to codewords
Indexing: mapping codewords to information
Isomorphism between information (ring) and codewords (group)
Quantization and Modulo

Quantization Closest point in $\Lambda_s$:

$$Q_{\Lambda_s}(y) = \arg \min_{x \in \Lambda_s} \| x - y \|^2$$

Quantization has exponential complexity in general.
Quantization and Modulo

Voronoi region at origin
Quantization and Modulo

Modulo operation:

\[ y = x \mod \Lambda_s \]

\[ = x - Q_{\Lambda_s}(x) \]

find the image of \( x \) in \( \mathcal{V} \)
Real Addition with Lattice Codes

Recall the multiple-access scenario

- $c_1, c_2 \in \mathcal{C}$ are finite group elements
- $c_1 \oplus c_2 \in \mathcal{C}$ is well defined
- But, real addition in the channel:
  \[ c_1 + c_2 \notin \mathcal{C} \]
- Solution: $c_1 + c_2 \mod \Lambda_s \in \mathcal{C}$
Real Addition with Lattice Codes

Example $A_2/3A_2$

$c_1 + c_2 \mod \Lambda_s$

$c_1 + c_2$
Encoding and Indexing

Index $b$ is information: $b = [b_1 \ b_2 \ \cdots \ b_n]^t$, 
where $b_i \in \{0, 1, \cdots, K - 1\}$.

given index $b$, find $x \in \mathcal{C}$

given $x \in \mathcal{C}$, find index $b$

$b \xrightarrow{Encoding} x$

$x = \text{enc}(b)$

$x \xrightarrow{Indexing} b$

$b = \text{enc}^{-1}(x) = \text{index}(x)$
Encoding Parallelotope

Example: $A_2/4A_2$

Index $b$ is information $b_i \in \{0, 1, 2, 3\}$:

$$x = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

(generator matrix)
Encoding the Voronoi Region

Two steps:

1. Parallelotope encoding
   \[ x = G \cdot b \]

2. Modulo operation
   \[ x = G \cdot b - Q_{A_s} (G \cdot b) \]
Encoding the Voronoi Region

Two steps:

1. Parallelotope encoding
   \[ x = G \cdot b \]

2. Modulo operation
   \[ x = G \cdot b - Q_{\Lambda_s}(G \cdot b) \]
Information (indices) \( b_i \in \mathbb{Z}/K\mathbb{Z} \) form a ring with operation \( \oplus, \otimes \) (integers modulo \( K \)).

Lattice codewords \( x \in \mathcal{C} \) for a group with operation \( + \) (vector addition modulo \( \Lambda_s \)).

Easy to show there is isomorphism:

\[
\text{enc}(b_1 \oplus b_2) = \text{enc}(b_1) + \text{enc}(b_2) \quad \text{or} \\
\text{index}(x_1) \oplus \text{index}(x_1) = \text{index}(x_1 + x_2)
\]
Group Isomorphism for PLNC

Simple multiple access channel

Assuming successful decoding:
- Decoder produces $x_1 + x_2$ (not $x_1$, $x_2$ individually)
- Indexing produces $b_1 \oplus b_2$ (not $b_1$, $b_2$ individually)
- Highly suitable for network coding
And now for something new…

Nested lattice codes with non-self-similar lattices

- High dimension lattices (LDLC, etc.): excellent coding gain, computationally hard to perform shaping,
- Low dimension lattices (E8, Barnes-Wall): Good shaping gain with efficient algorithms, not very good coding gain.
Nested lattice codes with non-self-similar lattices

Proposed method. Construct a quotient group:

\[ \Lambda_c / \Lambda_s \]

High-dimension lattice:
\( n = 1,000 \) to \( 10^5 \)
E8, Barnes-Wall, etc. lattice
\( n = 8, 16 \)
Nested lattice codes with non-self-similar lattices

Proposed method. Construct a quotient group:

\[ \Lambda_c / \Lambda_s \times \cdots \times \Lambda_s \]

High-dimension lattice: 
\[ n = 1,000 \text{ to } 10^5 \]

E8, Barnes-Wall, etc. lattice 
\[ n = 8, 16 \]
Sufficient Conditions to form a Group

Given a coding lattice $\Lambda_c$ and a shaping lattice $\Lambda_s$, we need to test the condition $\Lambda_s \subseteq \Lambda_c$.

Let $G_s$ be a $n \times n$ generator matrix for $\Lambda_s$.

Let $H = G^{-1}$ be the check matrix for $\Lambda_c$

**Lemma** $\Lambda_s \subseteq \Lambda_c$ if and only if $H \cdot G_s$ is a matrix of integers.

Easy to design $\Lambda_c$ such that $\Lambda_c \subseteq \Lambda_s$.
Achieving $\Lambda_s \subset \Lambda_c$ is easy.

Encoding/indexing is nontrivial.

Example for $n = 2$:

$$G_s = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} \quad \leftarrow \quad \Lambda_s$$
Achieving $\Lambda_s \subset \Lambda_c$ is easy.

Encoding/indexing is nontrivial.

Example for $n = 2$:

$$G_s = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} \quad \Lambda_s$$

$$G_c = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} \quad \Lambda_c$$

$$\left( G_c^{-1} = \begin{bmatrix} 1 & -1/4 \\ 1/2 & 1 \end{bmatrix} \right)$$

Note:

- $\Lambda_s \neq K\Lambda_c$ not self similar
- but $\Lambda_s \subset \Lambda_c \Rightarrow \Lambda_c/\Lambda_s$
Indexing Non-Nested Lattice Codes

Number of codewords:
\[
\frac{\det(G_s)}{\det(G_c)} = 36
\]

Natural candidate:
\[
\begin{align*}
b_1 &\in \{0, 1, 2, 3, 4, 5\} \\
b_2 &\in \{0, 1, 2, 3, 4, 5\}
\end{align*}
\]

Parallelootope encoding step:
\[
G_c b = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}
\]

Do these points form coset leaders?
Encoding Step 2:

\[ x = Gb - Q_{A_s}(Gb) \]

**No!** Coset leaders not formed.

What about a change of basis?
Finding a Basis Suitable for Encoding

We want to transform the basis of $G_c$:

$$G'_c = G_c W$$

where $W$ is has integer entries and $\det W = 1$. New basis is:

$$G'_c = \begin{bmatrix} \frac{g_1}{M_1} & \frac{g_2}{M_2} & \cdots & \frac{g_{n-1}}{M_{n-1}} & q \end{bmatrix}$$

where $q$ is some vector to be found. Find $W$:

$$(G_c)^{-1} \cdot G'_c = W$$

$$= \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1,n-1} & z_1 \\ w_{21} & w_{22} & \cdots & w_{2,n-1} & z_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n-1} & z_n \end{bmatrix}$$

Then $\det W = 1$ is a **linear diophantine equation** in $z_1, z_2, \ldots, z_n$. 
Indexing Non-Nested Lattice Codes Using a Suitable Basis

\[
\begin{bmatrix}
1 & -1/4 \\
1/2 & 1
\end{bmatrix} \cdot \begin{bmatrix}
4/3 & q_1 \\
4/3 & q_2
\end{bmatrix} = \begin{bmatrix}
1 & z_1 \\
2 & z_2
\end{bmatrix}
\]

\[
\det W = 1 \Rightarrow 1z_2 - 2z_1 = 1 \text{ has numerous solutions.}
\]
Summary – Physical Layer Network Coding

PLNC:

• Technique for cooperative wireless networks
• Exploit network coding to increase capacity
• Lattices: real codes to correct errors, shaping gain
• Remove noise first, and interference later
• Compute-and-Forward relaying also deals with fading
Recommended Reading


G. David Forney, Lecture notes for Principles of Digital Communications II Course at MIT http://dspace.mit.edu/

Ram Zamir, *Lattice Coding for Signals and Networks*, Cambridge Univ Press, September 2014