Lattice Network Codes Based on Eisenstein Integers for Wireless Multiple-Access Relay Networks

Jinhong Yuan

原進宏

University of New South Wales (UNSW)

Chinese University of Hong Kong (CUHK)

22.02.2012
Outlines

• Physical-layer Network Coding (PNC)
• Compute-and-forward (CF)
• Lattice Network Coding (LNC)
• Design Examples
• Union Bound Estimation (UBE)
• Conclusion
PNC

- Physical Layer Network Coding (PNC): decode the modulo-two sum of the two transmitted signals.
- Can enhance the throughput of a binary-input two-way relay channel (TWRC) [1]
- Approach the capacity upper bound of a Gaussian TWRC within ½ bits [2]

Compute-and-Forward

- Nazer-Gastpar proposed a new strategy: Compute-and-forward (CF) for a Gaussian multiple access relay channel (MARC).
- CF is an extension of PNC: multiple-user/q-ary input/fading
- **Key idea:**
  - relay decodes a linear function of the transmitted messages
  - rather than decoding each user’s message individually

**Compute-and-Forward**

- Map the noisy linear **C-combined** signal from the channel
  \[ y = \sum_{i=1}^{L} h_i x_i + z \]
  to a linear (integer) function (network coding)
  \[ u = \sum_{i=1}^{L} a_i w_i \]

- **Underlying principle:** based on linear nested lattice codes
  - The integer combinations of the lattice points (codewords) is another lattice point (codeword).
  - It can be mapped back to the linear combinations of the messages \( u \) over the finite field.
Lattice

A lattice $\Lambda$ is a discrete subset of n-space that has the group property.

An integer lattice: $\mathbb{Z}^n$

A lattice can be viewed as the linear transformation of the integer lattice $\mathbb{Z}^n$ by a generator matrix $B$ over $\mathbb{R}^{n \times n}$.

\[ \Lambda = B\mathbb{Z}^n \]
Lattice

• By the group property, any translation $\Lambda + x$ by a lattice point $x$ is just $\Lambda$, i.e. shift invariant.

• **Closed** under addition: $\lambda_1, \lambda_2 \in \Lambda \implies \lambda_1 + \lambda_2 \in \Lambda$.

• **Symmetric:** $\lambda \in \Lambda \implies -\lambda \in \Lambda$

• Implies: Lattice is **geometrically uniform** in Euclidean distance
  – Every point has the same number of neighbors at each distance.
  – All decision regions of a minimum-distance decoder are congruent.

\[ Z^2 \quad BZ^2 \]
Lattice

- Nearest neighbor quantizer (decoder): send a vector $x$ to a nearest lattice point in terms of the Euclidean distance.

$$\mathcal{D}_Λ(x) \triangleq \arg\min_{\lambda \in Λ} ||x - \lambda||$$

- The Voronoi region of a lattice point: the set of all points that quantize to the lattice point.

- Fundamental Voronoi region $\mathcal{V}$: the sets of points quantize to the origin.

$$\mathcal{V} = \{x : Q_Λ(x) = 0\}$$
Nested Lattice

• Consider a sublattice $\Lambda'$ of lattice $\Lambda$. They are nested as $\Lambda' \subset \Lambda$.
  
  – **Fine lattice** $\Lambda$
  – **Coarse lattice** $\Lambda'$

• **Nested Lattice code**: The set of lattice points of the fine lattice $\Lambda$ in the fundamental Voronoi region $\nu$ of the coarse lattice $\Lambda'$.

• The region $\nu$ is also called the **shaping region** of the code.

• The code rate

\[
R = \frac{1}{n} \log_2 \frac{V(\Lambda')}{V(\Lambda)}
\]
Nested Lattice Encoding

- Define a linear **code generator** $G$ and **Lattice generator** $B$
- Generate codeword $Gw$ for message $w$
- Map the scaled down version $rGw$ into the fundamental Voronoi region $(hypercube)$ $\mathcal{V} = [-1/2, 1/2)^n$
- Generate **fine lattice** $t=BrGw$
- Generate **coarse lattice** $\Lambda' = BZ^n$
- Generate a random **dither vector** $d$ uniformly over $\mathcal{V}$
- Transmit a **dithered codeword** $x = [ t+d ] \mod \Lambda'$
Nested Lattice Encoding/Decoding

- Encoders use the same nested lattice codes, transmit dithered codewords
  \[ x_i = [t_i + d_i] \mod \Lambda' \]
  \[ = [B_r G w_i + d_i] \mod \Lambda' \]

- Decoder scales by \( \alpha \)

Removes dithers

\[
\left[ \alpha y - \sum_i q_i d_i \right] \mod \Lambda'
\]

\[
= \left[ \alpha \left( \sum_i h_i x_i + z \right) - \sum_i q_i d_i \right] \mod \Lambda'
\]

\[
= \left[ \sum_i q_i x_i + \sum_i (\alpha h_i - q_i) x_i + \alpha z - \sum_i q_i d_i \right] \mod \Lambda'
\]

\[
= \left[ \sum_i q_i [t_i + d_i] \mod \Lambda' + \sum_i (\alpha h_i - q_i) x_i + \alpha z - \sum_i q_i d_i \right] \mod \Lambda'
\]

\[
= \left[ \sum_i q_i t_i + \sum_i (\alpha h_i - q_i) x_i + \alpha z \right] \mod \Lambda'
\]  

- Recovers linear equation (network code)

\[
\mathbf{u} = \left[ \sum_i q_i t_i \right] \mod \Lambda'
\]

\[
= \sum_i a_i w_i
\]

Effective noise: \( n = \sum_i (\alpha h_i - q_i) x_i + \alpha z \)
Compute-and-Forward

Effective noise: $n = \sum_i (\alpha h_i - q_i)x_i + \alpha z$

Minimizing the effective noise by choosing $\alpha$ to be MMSE coefficient

$$\alpha = \frac{P h^* a}{1 + P \|h\|^2}$$

The computation rate

$$R(h, a) = \log_2^+ \left( \|a\|^2 - \frac{P |h^* a|^2}{1 + P \|h\|^2} \right)$$
Compute-and-Forward

Performance of Gaussian TWRC

From: Nazer/Gastpar
Compute-and-Forward

\[ h = [2.1 \ 1.4] \]

\[ a = [3 \ 2] \]

Effective Noise: \( N + P |h-a|^2 \)

From: Nazer/Gastpar
Compute-and-Forward

\[ \alpha h = [\alpha 2.1 \quad \alpha 1.4] \]

\[ a = [3 \quad 2] \]

Effective Noise: \( \alpha^2 N + P |\alpha h - a|^2 \)

From: Nazer/Gastpar
Map back to equation of message symbols over the field:

\[ \alpha h = [\alpha 2.1 \quad \alpha 1.4] \]

\[ a = [3 \quad 2] \]

Effective Noise: \( \alpha^2 N + P |\alpha h - a|^2 \)  

From: Nazer/Gastpar
Compute-and-Forward

- A **theoretic guideline** as it assumes an infinite sequence of good lattice partition.

- **Map message** to a lattice point
  \[ t_i = \phi(w_i) \]

- Transmit **dithered codeword**
  \[ x_i = \left[ t_i + d_i \right] \mod \Lambda' \]

- The decoder recovers
  \[ \sum_i q_i t_i \mod \Lambda' \]

- Map it back to the linear combination of the messages
  \[ \sum_i a_i w_i = \phi^{-1}\left( \sum_i q_i t_i \mod \Lambda' \right) \]

- **Question:**
  - How to design the mapping functions?
  - How to implement modulo operation in n-space?
Lattice Network Coding

• A general algebraic framework proposed by Feng/Silva/Kschischang to design and implement practical compute-and-forward scheme using finite dimension lattice partition.

• It makes direct connection between the CF strategy and module theory.

• Using the algebraic properties of principal ideal domain (PID), it links the C-linear combination operation performed by the channel

\[ y = \sum_i h_i x_i + z \]

and the R-linear combination operation in the message space for the network coding

\[ \sum_i a_i w_i \]

Lattice Network Coding

• Let R be a discrete subring of C forming a principal ideal domain PID (e.g., integer numbers, Gaussian integers Z[i])

• Define an R-lattice \( \Lambda = \left\{ rG_\Lambda : r \in R^n \right\} \) (R-module) and its sublattice of \( \Lambda' \).

• The set of all the cosets of \( \Lambda' \) in \( \Lambda \), denoted by \( \Lambda / \Lambda' \), forms an R-lattice partition of \( \Lambda \). The message space \( W=\Lambda / \Lambda' \). (Figure)

• Define a linear labelling
  \( \phi^{-1}: \Lambda \rightarrow \Lambda / \Lambda' \)
  taking a lattice point \( \lambda \) in \( \Lambda \), map to a coset \( \lambda + \Lambda' \) of \( \Lambda' \) in \( \Lambda \).

• Define an embedding map
  \( \phi: \ W \rightarrow \Lambda \)
  embedding each message to a lattice point in the same coset.
Lattice Network Coding

- The encoder maps a message $w=\lambda+\Lambda'$ to a coset leader, using the embedding map.

$$x_i = \varepsilon(w_i) = \phi(w_i) - D_{\Lambda'}\left(\phi(w_i)\right)$$

- The decoder estimates an R-linear combination

$$\sum_i q_i x_i$$

from the C-linear combination

$$y = \sum_i h_i x_i + z$$

and maps the R-linear combination to a coset $\Lambda/\Lambda'$ by using linear labelling

$$\sum a_i w_i = \phi^{-1}\left(D_{\Lambda}(\alpha y)\right)$$

- R is a subring of C, the linear labelling induces a nature bridge between the C-linear combining and the R-linear combining in the message space.
Lattice Network Coding

How to **construct linear labelling** $\phi^{-1}: \Lambda \to \Lambda / \Lambda'$ ?

**Theorem** (Feng/Silva/Kschischang)

Let $R$ be a PID and $\Lambda / \Lambda'$ be a finite $R$-lattice partition. There exist generator matrices for $\Lambda$ and $\Lambda'$ satisfying

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

where $\pi_1 | \pi_2 | \cdots | \pi_k$ are the invariant factors of $\Lambda / \Lambda'$.

And the linear labelling is represented by a direct sum of modules $R/\pi$

$$\phi^{-1}: \Lambda \to \Lambda / \Lambda' \cong R / (\pi_1) \oplus R / (\pi_2) \oplus L \oplus R / (\pi_k)$$

$$\phi^{-1}(rG_{\Lambda}) = (r_1 + \pi_1, r_2 + \pi_2, L, r_k + \pi_k)$$

**Implies:**

- Construct high-D lattice from low-D lattice.
- We only consider linear labelling for 1-D baseline lattice $R/\pi$. 
LNC Based on Gaussian Integer

- **Gaussian integer** \( Z[i] = \{a + bi : a, b \in \mathbb{Z}\} \)
- Discrete subring of the complex numbers.

**Example.**

Consider a lattice \( Z[i] \) and its sublattice \( \beta Z[i] \), where \( \beta = 2 + 3i \) (Gaussian integer).

A finite field \( F_{13} \) is isomorphic to \( Z[i] / \beta Z[i] \).

The message space \( W = (Z[i] / \beta Z[i])^k \)

The shaping is a rotated hypercube in \( C^n \).

**The encoder** maps a message \( w = \lambda + (Z[i] / \beta Z[i])^k \) into its coset leader.

**The decoder** uses the linear labelling

\[
\phi^{-1}(r) = ((r_i - \lfloor r_i / \beta \rfloor \times \beta) + \beta, \text{ L }, (r_k - \lfloor r_k / \beta \rfloor \times \beta) + \beta)
\]
Union bound Estimation (UBE) of the error probability for hypercube shaping

\[ P_e(h, a) \approx K(\Lambda/\Lambda') \exp \left( -\frac{d^2(\Lambda/\Lambda')}{4N_0Q(\alpha, a)} \right) \]

where

\[ Q(\alpha, a) = |\alpha|^2 + SNR \|\alpha h - a\|^2 \]

The effective noise is \( N_0 Q(\alpha, a) \).

The minimum inter-coset distance of \( \Lambda/\Lambda' \): \( d(\Lambda/\Lambda') \).

It is also called the length of the shortest vectors in the set difference \( \Lambda \setminus \Lambda' \)

The number of shortest vectors: \( K(\Lambda/\Lambda') \)

The kissing number.
LNC Based on Gaussian Integer

Union bound Estimation (UBE) of the error probability

\[ P_e(h, a) \approx K(\Lambda / \Lambda') \exp \left( -\frac{d^2(\Lambda / \Lambda')}{4N_0Q(\alpha, a)} \right) \]

\[ = K(\Lambda / \Lambda') \exp \left( -\frac{\gamma_c(\Lambda / \Lambda')3\text{SENR}_{\text{norm}}}{2} \right) \]

The normalized signal-to-effective-noise ratio

\[ \text{SENR}_{\text{norm}} = \frac{\text{SENR}}{2^R} = \frac{\text{SNR}}{2^R Q(\alpha, a)} \]

The nominal coding gain:

\[ \gamma_c(\Lambda / \Lambda') = \frac{d^2(\Lambda / \Lambda')}{V(\Lambda)^{1/n}} \]

Measures the increase in density of \( \Lambda \) over the baseline uncoded hypercube lattice. The nominal coding gain for the baseline system is 0 dB.
LNC Based on Eisenstein Integer

- **Eisenstein integer** \( Z[w] = \{a + bw : a, b \in \mathbb{Z}\} \quad w = \left( -1 + \sqrt{-3} \right) / 2 \)
- \( Z[w] \) forms a PID.
- Lattice partitions over \( Z[w] \) enrich the candidates of finite fields.
- It has six Eisenstein units.
- The Voronoi region of \( Z[w] \) lattice is a regular hexagon (better shaping region).
- It has efficient division algorithms, essential for practical encoder/decoder.
- Optimum lattice/packing in 2-D.
Example.

Consider a lattice $\mathbb{Z}[w]$ and its sublattice $r\mathbb{Z}[w]$, where $r=4+3w$ (Eisenstein integer).

A finite field $F_{13}$ is isomorphic to $\mathbb{Z}[w]/r\mathbb{Z}[w]$.

The message space $W=(\mathbb{Z}[w]/r\mathbb{Z}[w])^k$

The shaping is a rotated product of $n$ regular hexagons in $\mathbb{C}^n$. 

(a) $\mathbb{Z}[i]$  
(b) $\mathbb{Z}[\omega]$
LNC Based on Eisenstein Integer

**Quantizer** of a complex value $x$ to an Eisenstein Integer

$$D_\Lambda (x) = \arg \min \left\{ |x - \beta_i|^2 \right\}$$

$$\beta_1 = \left[ \text{Re}\{x\} \right] + \sqrt{-3} \left[ \text{Im}\{x\} / \sqrt{3} \right]$$

$$\beta_2 = \left[ \text{Re}\{x - w\} \right] + \sqrt{-3} \left[ \text{Im}\{x - w\} / \sqrt{3} \right] + w$$

For lattice partition $\mathbb{Z}[w]/r\mathbb{Z}[w]$, the encoder $\varepsilon: W \rightarrow \Lambda = \mathbb{Z}[w]$ uses a division algorithm.

**Example.**

Consider the lattice $\mathbb{Z}[w]$ and its sublattice $r\mathbb{Z}[w]$.

When $r=2$, $F_4$ is isomorphic to $\mathbb{Z}[w]/2\mathbb{Z}[w]$.

$W = \{0 + r\mathbb{Z}[w], \ 1 + r\mathbb{Z}[w], \ w + r\mathbb{Z}[w], \ 1 + w + r\mathbb{Z}[w]\}$.

One possible encoder:

$\varepsilon(W) = \{0, \ -1, \ -w, \ 1+w\}$
LNC Based on Eisenstein Integer

Theorem: Union bound Estimation (UBE) of the error probability

\[ P_e(h, a) \approx K(\Lambda / \Lambda') \exp \left( - \frac{d^2(\Lambda / \Lambda')}{4N_0Q(\alpha, a)} \right) \]

where

\[ Q(\alpha, a) = |\alpha|^2 + SNR \| \alpha h - a \|^2 \]

The minimum inter-coset distance of \( \Lambda / \Lambda' \): \( d(\Lambda / \Lambda') \).
It is also called the length of the shortest vectors in the set difference \( \Lambda \setminus \Lambda' \)

The number of shortest vectors: \( K(\Lambda / \Lambda') \)
The kissing number.
LNC Based on Eisenstein Integer

**Corollary: Union bound Estimation (UBE) of the error probability**

\[
P_e(h, a) \approx K(\Lambda / \Lambda') \exp \left( - \frac{d^2(\Lambda / \Lambda')}{4N_0Q(\alpha, a)} \right) \]

\[
= K(\Lambda / \Lambda') \exp \left( - \frac{\gamma_c(\Lambda / \Lambda')\gamma_s(\Lambda / \Lambda')3\text{SENR}_{\text{norm}}}{2} \right)
\]

The normalized signal-to-effective-noise ratio

\[
\text{SENR}_{\text{norm}} = \frac{\text{SENR}}{2^R} = \frac{\text{SNR}}{2^R Q(\alpha, a)}
\]

**The nominal coding gain:**

\[
\gamma_c(\Lambda / \Lambda') = \frac{d^2(\Lambda / \Lambda')}{V(\Lambda)^{1/n}}
\]

Measures the increase in density of \( \Lambda \) over the baseline uncoded hypercube lattice.
LNC Based on Eisenstein Integer

Corollary: Union bound Estimation (UBE) of the error probability

\[ \begin{align*}
P_e(h, a) &\approx K(\Lambda / \Lambda') \exp \left( -\frac{d^2(\Lambda / \Lambda')}{4N_0 Q(\alpha, a)} \right) \\
&= K(\Lambda / \Lambda') \exp \left( -\frac{\gamma'_c(\Lambda / \Lambda')\gamma'_s(\Lambda / \Lambda')3\text{SENR}_{\text{norm}}}{2} \right)
\end{align*} \]

Second Moment (average energy per dimension of a uniform PDF):

\[ P(\Lambda) = \int_{V} \frac{\|x\|^2}{n} p(x) dx = \int_{V} \frac{\|x\|^2}{n V(\Lambda)} dx \]

Normalized Second Moment
(dimensionless, invariant to scaling, orthogonal transformation and Cartesian products):

\[ G(\Lambda) = \frac{P(\Lambda)}{V(\Lambda)^{1/n}} \]

The shaping gain:

\[ \gamma'_s(\Lambda / \Lambda') = \frac{G(\text{hypercube})}{G(\Lambda)} = \frac{1/6}{G(\Lambda)} = \frac{V(\Lambda)^{1/n}}{6P(\Lambda)} \]

Measures how much less is the average energy of \( \Lambda \) relative to a hypercube.
LNC Based on Eisenstein Integer

Consider LNC based on Eisenstein integer $\beta$ and lattice partition $\mathbb{Z}[w]/\beta\mathbb{Z}[w]$

The baseline system has a nominal coding gain

$$\gamma_c(\Lambda / \Lambda') = \frac{2\sqrt{3}}{3} = 0.625 \text{ dB}$$

The shaping gain

$$\gamma_s(\Lambda / \Lambda') = \frac{3\sqrt{3}}{5} = 0.167 \text{ dB}$$

Corollary:

For an LNC by complex construction $A$ over $\mathbb{Z}[w]/\pi\mathbb{Z}[w]$, where $\pi$ is an Eisenstein prime, the nominal coding gain based

$$\gamma_c(\Lambda / \Lambda') = \frac{2\sqrt{3}}{3} \frac{w_E^{\min}(C)}{|\pi|^{2(1-k/n)}}$$

Union bound Estimation (UBE) of the error probability

$$P_e(h, a) \approx K(\Lambda / \Lambda') \exp\left(-\frac{9}{5} \frac{w_E^{\min}(C)\text{SENR}_{\text{norm}}}{|\pi|^{2(1-k/n)}}\right)$$
LNC Based on Eisenstein Integer

Compare two LNC baseline systems’ performance
Two transmitter and a single relay.
Eisenstein prime $r$ and lattice partition $\mathbb{Z}[w]/r\mathbb{Z}[w]$  
Gaussian prime $\beta$ and lattice partition $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$
LNC Based on Eisenstein Integer

**Design Examples** (maximize the coding gain)

Convolutional codes with rate $\frac{1}{2}$ over lattice partition $\mathbb{Z}[i]/\beta \mathbb{Z}[i]$, $\beta=2+3i$

<table>
<thead>
<tr>
<th>$\nu$</th>
<th>$g(D)$</th>
<th>$\gamma_c$</th>
<th>$w_{\text{min}}$</th>
<th>$K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$[1+2D, 2+(1+i)D]$</td>
<td>2.22 (3.36 dB)</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>$[1+D+2iD^2, (-1-i)+(-1+i)D+(-1-i)D^2]$</td>
<td>3.33 (5.22 dB)</td>
<td>12</td>
<td>4</td>
</tr>
</tbody>
</table>

Convolutional codes with rate $\frac{1}{2}$ over lattice partition $\mathbb{Z}[w]/r\mathbb{Z}[w]$, $r=4+3w$

<table>
<thead>
<tr>
<th>$\nu$</th>
<th>$g(D)$</th>
<th>$\gamma_c$</th>
<th>$w_{\text{min}}$</th>
<th>$K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$[1+D, (-1+w)+(2+w)D]$</td>
<td>2.56 (4.09 dB)</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>$[1+D+(-1+w)D^2, (-1+w)+(1-w)D+(1+w)D^2]$</td>
<td>3.84 (5.85 dB)</td>
<td>12</td>
<td>24</td>
</tr>
</tbody>
</table>
Summary

• Reviewed physical-layer network coding and compute-and-forward

• Investigated the lattice network coding based on Eisenstein integer

• Quantizer/encoding algorithms

• Derived Union bound estimation in a unified way

• A few code examples

• LNC based on Eisenstein integer has a high nominal coding and shaping gain.

Open problems:

• Lattice-reduction algorithms to find optimal combination coefficients
• Design more power codes
• Other Lattice Constructions (Construction D algorithm)
Acknowledgement

Qifu Tyler Sun, CUHK

Kenneth W. Shum, CUHK

INC
Thank You!