Generalized Voronoi Constellations

Brian M. Kurkoski
Japan Advanced Institute of Science and Technology

November 26, 2015
Symposium on Information Theory and Its Applications (SITA2015)
Kurashiki, Okayama, Japan
Usefulness of Lattice Codes

Lattice codes can achieve the capacity of AWGN channel [Erez and Zamir ’04] Information theoretic results and physical layer network coding using lattices:

- Lattices for relay channel e.g. [Song-Devroye ’13]
- Two-way (Bidirectional) relay channel e.g. [Wilson et al.]
- Compute-forward relaying [Nazer-Gastpar ’11]

“Physical layer network coding”

How to construct practical, capacity-approaching lattices?
A lattice $\Lambda$ is a linear additive subgroup of $\mathbb{R}^n$.

Given a basis $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$, the lattice consists of all points

$$\begin{bmatrix}
\mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n
\end{bmatrix} \begin{bmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{bmatrix}$$

for $b_i \in \mathbb{Z}$.

Given $\Lambda$, there are arbitrarily many possible bases.
Voronoi Constellations or Nested Lattice Codes

Conway and Sloane [IT 83] described Voronoi constellations

- $\Lambda$ is a lattice
- $M\Lambda$ is scaled by $M$.
- $\Lambda/M\Lambda$ is a quotient group
- coset leaders Euclidean-space code

Also called nested lattice codes
Physical Layer Network Coding: Signals Add Over the Air

User 1 has $w_1$
User 2 has $w_2$
Relay wants $w_1 + w_2$
Two Users Transmit to Relay

\[ x_1 = \text{enc}(w_1) \]

\[ x_2 = \text{enc}(w_2) \]
\[ z = x_1 \oplus x_2 \]
Background Summary

Lattices are codes over the real numbers.

Network coding for wireless networks: signals add over the air: physical layer network coding

Voronoi constellations (nested lattice codes) have three properties:

1. Coding lattice $\Lambda$ — good for error correction

2. Shaping lattice $M\Lambda$ —
   - As $n \to \infty$ Voronoi region is sphere like
   - A sphere achieves optimal AWGN input distribution (and Shannon capacity). Optimal 1.53 dB shaping gain

3. Forms a quotient group required for physical layer network coding

Good for theoretical results, difficult to construct capacity-achieving codes
Contributions

Generalized Voronoi Constellations — Practical lattice codes

- Shaping lattice is not a scaled coding lattice:

  \[ \Lambda_c / \Lambda_s \]

  coding lattice \[ \rightarrow \] \[ \Lambda_c / \Lambda_s \] \[ \leftarrow \] shaping lattice

  is high dimension, high shaping gain
capacity-approaching efficient shaping algorithm

- Give necessary and sufficient condition so $\Lambda_c / \Lambda_s$ is a group
- Encoding for triangular coding matrices: easy
- Encoding for general coding matrices: not so easy
How to Design a Coding Lattice

Approach unconstrained lattice capacity, lattice dimension $n$ should be large

**Construction A and Construction D**
- Construction D using LDPC codes [Sadeghi et al IT 2006]
- Construction A using non-binary LDPC codes [Huang et al ISIT 2014]
- Construction D using polar codes [Yan et al ITW 2012]

Derive generator matrix $G$, and check matrix $H = G^{-1}$ from the design

**Low-Density Lattice Codes (LDLC lattices)**
- [Sommer et al, 2008]
- Spatially-coupled LDLCs [Uchikawa et al, ISIT 2012]

Design the $H$ matrix to be sparse and other easy conditions.
Ideally, want a shaping lattice with efficient maximum-likelihood decoding:
1. Lattices based on convolutional codes (Viterbi-based decoding)
2. Low-dimension lattices, E8, BW16, etc.

Shaping lattice is concatenation of low-dimension lattices:

\[
\Lambda_s \times \Lambda_s \times \cdots \times \Lambda_s
\]

\(\text{dimension } n\)
Shaping Gain for Well-Known Lattices

- **Sphere bound**

- **Lattice dimension**
  - $n$

Graph showing the shaping gain (dB) for different lattice dimensions, from $Z_1$ to $\Lambda_{24}$, with increasing complexity from left to right.
Basic Group Theory

If $G$ is a group, and $H \subseteq G$ is a subgroup then $G/H$ is a quotient group.

If $\Lambda_s \subseteq \Lambda_c \Rightarrow \Lambda_c/\Lambda_s$ is a quotient group.

Conway and Sloane: $\Lambda/MA$ is a quotient group.
Sublattice (subgroup)
\[ \Lambda_s = 2A_2 \]
Lattice (group) $\Lambda_c = A_2$
<table>
<thead>
<tr>
<th></th>
<th>$\mathbf{c}_0$</th>
<th>$\mathbf{c}_1$</th>
<th>$\mathbf{c}_2$</th>
<th>$\mathbf{c}_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbf{c}_0$</td>
<td>$\mathbf{c}_0$</td>
<td>$\mathbf{c}_1$</td>
<td>$\mathbf{c}_2$</td>
<td>$\mathbf{c}_3$</td>
</tr>
<tr>
<td>$\mathbf{c}_1$</td>
<td>$\mathbf{c}_1$</td>
<td>$\mathbf{c}_0$</td>
<td>$\mathbf{c}_3$</td>
<td>$\mathbf{c}_2$</td>
</tr>
<tr>
<td>$\mathbf{c}_2$</td>
<td>$\mathbf{c}_2$</td>
<td>$\mathbf{c}_3$</td>
<td>$\mathbf{c}_0$</td>
<td>$\mathbf{c}_1$</td>
</tr>
<tr>
<td>$\mathbf{c}_3$</td>
<td>$\mathbf{c}_3$</td>
<td>$\mathbf{c}_2$</td>
<td>$\mathbf{c}_1$</td>
<td>$\mathbf{c}_0$</td>
</tr>
</tbody>
</table>

4 cosets. Coset containing $\mathbf{c}_0$, $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$. 
The Subgroup Condition

- Shaping lattice $\Lambda_s$ has generator matrix $G_s$.
- Coding lattice $\Lambda_c$ has check matrix $H_c$.

Lemma Let $\Lambda_s$ have an all-integer generator matrix $G_s$. $\Lambda_s \subseteq \Lambda_c$ if and only if $H_c G_s$ is a matrix of integers.

- Simple test for $\Lambda_s \subseteq \Lambda_c$.
- If $\Lambda_s \subseteq \Lambda_c \Rightarrow$ quotient group $\Lambda_c/\Lambda_s$ exists, and is a candidate for physical layer network coding.
The Subgroup Condition: Example

- dimension $n = 8$ coding lattice $\Lambda_c$ is LDLC-style

- shaping lattice $\Lambda_s$ on $D_4$

\[
\begin{bmatrix}
1 & 0 & 0 & \frac{1}{2} & 0 & 0 & -\frac{1}{4} & 0 \\
\frac{1}{4} & 1 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \\
0 & \frac{1}{2} & 1 & 0 & 0 & 0 & 0 & \frac{1}{4} \\
0 & 0 & \frac{1}{4} & 1 & 0 & 0 & -\frac{1}{2} & 0 \\
\frac{1}{2} & 0 & 0 & 0 & 1 & -\frac{1}{4} & 0 & 0 \\
0 & 0 & \frac{1}{2} & \frac{1}{4} & 0 & 1 & 0 & 0 \\
0 & -\frac{1}{4} & 0 & 0 & \frac{1}{2} & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -\frac{1}{4} & \frac{1}{2} & 0 & 1 \\
\end{bmatrix}
\]  
\begin{bmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -4 & 4 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -4 & 8 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -4 & 4 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -4 & 4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -4 & 8 \\
\end{bmatrix}
\]  
= matrix of integers

coding: LDLC $H_c$

shaping $4D_4 \times 4D_4$

- Condition is satisfied. Thus $\Lambda_c/\Lambda_s$ is a quotient group.
Encoding $\Lambda_c/\Lambda_s$

Encoding is mapping information to lattice points $\Lambda_c/\Lambda_s$.

For Conway and Sloane, indexing $\Lambda/M\Lambda$ is easy:

$$\{0, 1, \cdots, M - 1\}^n \rightarrow \Lambda/M\Lambda$$

For $\Lambda_c/\Lambda_s$ satisfying the subgroup condition

1. If coding check matrix $H_c$ is triangular, then indexing is also easy

2. If $H_c$ is full, then indexing is harder.
1. Encoding When $H_c$ is Triangular

$g_{ii}$ are diagonal elements of $G_s$, $h_{ii}$ are diagonal elements of $H_c$, then:

information is $\{0, 1, \cdots, g_{ii}h_{ii}\}$

and encoding info to $\Lambda_c/\Lambda_s$ is straightforward.

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & \frac{1}{4} & 0 & 1 & 0 & 0 \\
0 & -\frac{1}{4} & 0 & 0 & \frac{1}{2} & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -\frac{1}{4} & \frac{1}{2} & 0 & 1 \\
\end{bmatrix} \quad \begin{bmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -4 & 4 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -4 & 8 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -4 & 4 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -4 & 4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -4 & 8 \\
\end{bmatrix}
\]

\text{coding } H_c \quad \text{shaping } G_s
Encoding Lattice Codes, Conway and Sloane Style

Easy when $\Lambda_s = M\Lambda_c$ (Conway and Sloane 1983). Example:

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

$$G_c = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} (\Lambda_c)$$

$\Lambda_s = 4\Lambda_c$ nested lattice code
Encoding Lattice Codes, Conway and Sloane Style

Easy when $\Lambda_s = M\Lambda_c$ (Conway and Sloane 1983). Example:

\[
G_s = \begin{bmatrix}
4 & 0 \\
4 & 8
\end{bmatrix} (\Lambda_s)
\]

\[
G_c = \begin{bmatrix}
1 & 0 \\
1 & 2
\end{bmatrix} (\Lambda_c)
\]

$\Lambda_s = 4\Lambda_c$ nested lattice code
Information is $b_i \in \{0, 1, 2, 3\}$,

Indexing Step 1:

$$Gb = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$$

(clearly these points form coset representatives)
Codebook is coset representatives inside Voronoi region for $\Lambda_s$ around 0:

Indexing Step 2:

$$x = Gb - Q_{\Lambda_s}(Gb)$$
2. Encoding When $H_c$ is Full Matrix

Weakness of $H_c$ triangular:

- $H_c$ may not be available in triangular form
- triangular form reducing coding gain or rate.

If $H_c$ full:

- Give conditions under which encoding is possible
- requires solving a diophantine equation
What if the lattices are not nested? Recall we want to use distinct lattices for coding and shaping.

Example:

\[
G_s = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} (\Lambda_s)
\]

\[
G_c = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} (\Lambda_c)
\]

\[
G_c^{-1} = \begin{bmatrix} 1 & -1/4 \\ 1/2 & 1 \end{bmatrix}
\]

Not a nested lattice code!
Number of codewords:

\[ \frac{\det(G_s)}{\det(G_c)} = 36 \]

Natural candidate:

\[ b_1 \in \{0, 1, 2, 3, 4, 5\} \]
\[ b_2 \in \{0, 1, 2, 3, 4, 5\} \]

Indexing Step 1:

\[ Gb = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \]

Do these points form coset representatives?
Indexing Step 2:

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

No! Coset representatives not formed.
Another candidate:

\[ b_1 \in \{0, 1, 2\} \]
\[ b_2 \in \{0, 1, 2, 3, \ldots, 11\} \]

Still, no coset representatives found

What about a change of basis for \( G_c \)?
Finding a Basis Suitable for Encoding

Transform the basis of $\Lambda_c$ from $G_c$ to $G'_c$ should “align” with $\Lambda_s$.

Basis transformation:

$$G'_c = G_c W$$

where $W$ is has integer entires 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.
Finding a Basis Suitable for Encoding

Find basis transformation \( W \):\

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

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

Then \( \det W = 1 \) is a linear diophantine equation in \( z_1, z_2, \ldots, z_n \).
Example

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

\[ \det W = 1 \]

\[ 1z_2 - 2z_1 = 1 \quad \leftarrow \text{diophantine equation} \]

\[ \{z_1, z_2\} = \{0, 1\} \quad \leftarrow \text{one of many solutions} \]
Encoding Non-Nested Lattice Codes Using a Suitable Basis

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

\[
\det W = 1 \Rightarrow 1z_2 - 2z_1 = 1 \text{ has numerous solutions.}
\]
Shaping gain means designing the codebook to have a sphere-like shape, to approximate the Gaussian input distribution of the AWGN channel.

For coding lattice (LDLC, Constuction A LDPC, etc) triangular matrix:

- No shaping/cubic is easy but no shaping gain.
- Shaping using E8, BW16, etc. is also easy. Gain 0.65 to 0.86 dB.
- A little bit of effort gives a big gain!
- But, triangular matrix lattices may not perform as well.

For a general (non-triangular) matrices:

- Shaping if we can solve a linear diophantine equation,
- Currently those coefficients get large quickly in $n$, practical solutions still needed.
LDLCs: 0.65 dB Gain Over Hypercube

0.15 dB better than self-similar shaping (using M-algorithm) and much lower complexity