Voronoi Constellations for High-dimensional Lattice Codes

Nuwan Ferdinand*, Matthew Nokleby# and Behnaam Aazhang¤

University of Toronto, Toronto, ON, Canada*
Wayne State University, Detroit, MI, USA#
Rice University, TX, USA¤
Why lattice codes?

- Lattices achieve the capacity of AWGN channels
- They are “easily” decoded
- Their algebraic structure is useful in network information theory

\[ \sum_{l=1}^{L} a_l x_l \mod \Lambda_s \]
Lattice codes in theory

• Capacity results employ two (or more) ensembles of “good” high-dimensional lattices

• Coding lattice: efficiently packed codewords

• Shaping lattice: efficient power-shaping region

• Codebook is the quotient group of coding and shaping lattices
Lattice codes in practice

- Suboptimal, finite-dimensional lattices
- Low-complexity shaping algorithms
- Leads to **coding** and **shaping** losses:
Practical, efficient coding lattices exist

- Low density lattice codes — coding loss of 0.6dB for block length $10^5$
at error probability $10^{-5}$
- Turbo lattices
- LDPC lattices
- Integer LDA lattices
What about practical shaping?

• Use hypercube shaping: 1.53dB loss
• Self-similar shaping: use scaled coding lattice as shaping lattice
• Several practical problems:
  ❖ Quantization step, involved in modulo operation, increases with the dimension of coding lattice
  ❖ The use of iterative lattice decoding algorithms does not, in general, converge for quantization
  ❖ Does not guarantee good shaping gains due to unknown Voronoi region, in general
This talk

• Shaping via concatenations of a low-dimensional lattice

• Proposed construction offers advantages:
  • Low-complexity shaping algorithm
  • We can choose the shaping lattice to have low loss
  • Preserve isomorphism with finite field
Lattices

• An $n$-dimensional lattice is a discrete subgroup of $\mathbb{R}^n$
• It is defined by $n$ basis vectors, which forms the generator matrix $G$

$$\Lambda = G\mathbb{Z}^n$$
Lattice definitions

• The shortest-distance lattice quantization is denoted by, $Q_{\Lambda_n}(x)$ which maps any point $x \in \mathbb{R}^n$ to the nearest point in $\Lambda_n$

$$Q_{\Lambda_n}(x) = \arg \max_{\lambda \in \Lambda_n} ||x - \lambda||$$

• The modulo-lattice operation with respect to $\Lambda_n$ returns the quantization error:

$$x \mod \Lambda_n = x - Q_{\Lambda_n}(x)$$
Lattice definitions

• Let $\mathcal{P}_n$ denote the fundamental parallelepiped region of $\Lambda_n$ with respect to a generator $G$:

$$\mathcal{P}_n = \{Gs|0 \leq s_i < 1\}$$

• There is a shifted parallelepiped region for each point of $\Lambda_n$. Any point in $\mathcal{P}_n$ is in exactly one such region.

• The fundamental Voronoi region, denoted by $\mathcal{V}_n \subset \mathbb{R}^n$, of $\Lambda_n$ is the set of points that are closer to $\lambda = 0$ lattice point than to any other lattice point.
Coding lattice structure

\[ G = \begin{bmatrix}
G_{11} & 0 & 0 & 0 & 0 & 0 \\
G_{21} & G_{22} & 0 & 0 & 0 & 0 \\
G_{31} & G_{32} & G_{33} & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & 0 \\
G_{(n/m)1} & \vdots & \vdots & \vdots & \ddots & 0 \\
G_{(n/m)(n/m)} & \vdots & \vdots & \vdots & \vdots & \ddots
\end{bmatrix} \]

- Break lattice into blocks of length m, m<<n
- Lower-triangular generator matrix
- \( G_{ij} = g_{i,m} \) for i=j, can have arbitrary structure for j < i
- LDLCs, LDA lattices, etc. have this structure
Shaping lattice structure

• Construct shaping lattice from low-dimensional lattice \( \Lambda_{s,m} \)
• Let \( \Theta \in \mathbb{R}^{m \times m} \) denote its generator matrix
• Generator matrix is lower-triangular and satisfies:

\[
g_r^{-1} \theta_{ii} \in \mathbb{Z}, \forall \ r \in 1, \ldots, n/m
\]

\[
\theta_{ij}/\theta_{jj} \in \mathbb{Z}, \quad \forall \ i
\]

• Well-known lattices such as scaled \( D_m, E_8, \) and \( BW_{16} \) satisfy these conditions.
Code construction - encoding

• Break encoding up into m-length blocks:

\[ \mathbf{b} \in \mathbb{Z}^n \]
\[ \mathbf{b} = \left[ (\mathbf{b}^1)^T, (\mathbf{b}^2)^T, \ldots, (\mathbf{b}^{n/m})^T \right]^T \]
\[ \mathbf{b}^r = (b^r_1, \ldots, b^r_m)^T \]
\[ b^r_i \in \{0, 1, \ldots, g_r^{-1} \theta_{ii} - 1\} \]

• where \( g_r^{-1} \theta_{ii} \) is the i-th diagonal element of the generator matrix \( g_r^{-1} \Theta \), which is related to the scaled shaping lattice \( g_r^{-1} \Lambda_{s,m} \).
Code construction-encoding

\[ b^r \in \mathbb{Z}^m \Leftrightarrow c^r \in g_r^{-1} \mathcal{P}_m \cap \mathbb{Z}^m \]

\[ f^r = \begin{pmatrix} \frac{b^r_1}{g_r^{-1}\theta_{11}} & \frac{b^r_2}{g_r^{-1}\theta_{22}} & \cdots & \frac{b^r_m}{g_r^{-1}\theta_{mm}} \end{pmatrix}^T \]

\[ f^r \in [0, 1)^m \]

\[ c^r = g_r^{-1} \Theta f^r \]

\[ c = [(c^1)^T (c^2)^T \ldots (c^{n/m})^T]^T \]
Code construction-encoding

\[ \mathbf{b}^r \in \mathbb{Z}^m \iff \mathbf{c}^r \in g_r^{-1} \mathcal{P}_m \cap \mathbb{Z}^m \]

\[ b_i^r \in \{0, 1, \ldots, g_r^{-1} \theta_{ii} - 1\} \]
We introduce a subtractive dither:

\[
\begin{align*}
a^r &= [0, 1]^m \\
d^r &= \Theta a^r \\
d &= [(d^1)^T (d^2)^T \ldots (d^{n/m})^T]^T
\end{align*}
\]
Code construction-encoding

• Next we select integer vector $q \in \mathbb{Z}^n$ to satisfy the shaping condition, which will be explained later.

• Next, $c - \tilde{G}^{-1}d - q$ is encoded block-wise using generator matrix $G$. Encoding starts at the first block of $c - \tilde{G}^{-1}d - q$ and continues sequentially.

$$x' = G(c - \tilde{G}^{-1}d - q)$$
Code construction-encoding

\[
\begin{align*}
q^r &= [q_{(r-1)m+1} \ldots q_{rm}]^T \in \mathbb{Z}^m \\
x'^r &= [x'_{(r-1)m+1} \ldots x'_{rm}]^T \in \mathbb{R}^m \\
c^r &= [c_{(r-1)m+1} \ldots c_{rm}]^T \in \mathbb{Z}^m \\
d^r &= [d_{(r-1)m+1} \ldots d_{rm}]^T \in \mathcal{P}_m
\end{align*}
\]

\[
s^r = [G_{r1}G_{r2} \ldots G_{r(r-1)}] \cdot [(k^1)^T(k^2)^T \ldots (k^{r-1})^T]^T \text{ where } k^r = c^r - g_r^{-1}d^r - q^r
\]

\[
x'^r = G_{rr}(c^r - g_r^{-1}d^r - q^r) + s^r = g_r c^r - d^r + s^r - g_r q^r.
\]
Code construction-encoding

\[ b^r \in \mathbb{Z}^m \]
Code construction-encoding

\[ e^r \in g_r^{-1} P_m \cap \mathbb{Z}^m \]

\[ b^n \in \mathbb{Z}^m \]
Code construction-encoding

\[ g_r c^r - d^r + s^r \]

\[ e^r \in g_r^{-1}P_m \cap \mathbb{Z}^m \]
Code construction-encoding

\[ g_r q^r = Q_{\Lambda_{s,m}} (g_r c^r - d^r + s^r) \]

\[ q^r = Q_{g_r^{-1} \Lambda_{s,m}} (\cdot) \in \mathbb{Z}^m \]

\[ g_r c^r - d^r + s^r \]
Code construction-encoding

\[ g_r \mathbf{q}^r = Q_{\Lambda_{s,m}}(g_r \mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r) \]
\[ \mathbf{q}^r = Q_{g_r^{-1}\Lambda_{s,m}}(\cdot) \in \mathbb{Z}^m \]

\[ g_r \mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r \]

\[ x'^r = g_r \mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r - Q_{\Lambda_{s,m}}(g_r \mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r) \]
\[ = [g_r \mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r] \mod \Lambda_{s,m}. \]
Decoding

\[ y = hx' + z, \]
\[ \hat{x} = Q_{\Lambda_e,n} \left( h^{-1}y + G\tilde{G}^{-1}d \right) \]
\[ w = c - q \]
\[ w^r = c^r - q^r \]
\[ w^r = g_r^{-1}\Theta f^r - q^r \]
\[ w^r = g_r^{-1}\Theta f^r - g_r^{-1}\Theta \tilde{q}^r \]
\[ g_r\Theta^{-1}w^r = f^r - \tilde{q}^r \]
\[ f^r = \left[ g_r\Theta^{-1}w^r \right] \mod Z^m \]
\[ b^r = g_r^{-1}\tilde{\Theta}\left[ g_r\Theta^{-1}w^r \right] \mod Z^m \]

\[ q^r \in g_r^{-1}\Lambda_{s,m} \quad \tilde{q}^r \in Z^m \]

\[ f^r \in [0, 1)^n \]
Complexity

- Complexity of the proposed scheme is linear with the dimension of high dimensional coding lattice:

\[ \mathcal{O} \left( n \left( \frac{c}{m} + d \right) \right) \]

Where
- \( n \) – dimensional of coding lattice
- \( c \) – complexity involved in quantization step using shaping lattice. For E8 lattice \( c=72 \).
- \( m \) – dimensional of shaping lattice. For E8 lattice \( m=8 \).
- \( d \) – number of non-zero elements in generator matrix of coding lattice. For LDLC, LDA, \( d=8 \).
Performance

• **Theorem:** The shaping loss of the full shaping lattice is the same as the shaping loss of $\Lambda_{s,m}$
  
  **Proof:** Taking Cartesian products does not affect the normalized second moment of a lattice.

• Can exploit the shaping properties of E8, BW16 lattices

• **Theorem:** The coding loss of the shaped codebook is the same as the unshaped coding lattice
  
  **Proof:** Follows from lower-triangular structure

• Can exploit the coding properties of LDLCs, LDA lattices
Algebraic structure for compute and forward

\[ y = \sum_{l=1}^{L} r_l x_l' + z \]

\[ v = \bigoplus_{l=1}^{L} a_l b_l \]
Mapping for compute and forward

\[
\phi^{-1}(\sum_{l=1}^{L} a_l x_l) \equiv \bigoplus_{l=1}^{L} a_l b_l \mod \mathbb{Z}^n
\]

where \( \bigoplus \) s modulo summation over \( \bar{G}^{-1} \Theta^n 1^n \)

\[
\phi^{-1}(u) = \bar{G}^{-1} \Theta^n \left( [\tilde{G}(\Theta^n)^{-1} G^{-1} u] \mod \mathbb{Z}^n \right)
\]
Which finite field?

• Compute-and-forward requires modulo summation over a prime field

• This requirement can be satisfied by designing shaping matrices such that $g_{ii}^{-1} \theta_{ii} = p^{l_i}$ where $p$ is a prime number and $l_i \in \mathbb{Z}$

• For lattices such as scaled $D_m, E_8$ and $BW_{16}$, the related prime number is $p = 2$

• Can experimentally design lattices for higher primes
Shaping gain-numerical results

![Graphs showing shaping gain results for different scenarios](image_url)
Symbol error performance: with LDLC as coding lattice.

Symbol error rate versus average SNR for Voronoi integers. For $n = 10^4$ and $R = 4.935$ bits/dimension.
Conclusion

• Codebook construction for high-dimensional lattice codes using the Voronoi region of a low-dimensional lattice

• Allows us to leverage high-performance coding lattices (LDA, LDLCs) and high-performance shaping lattices (E8, BW16)

• Low encoding complexity

• Permits mapping between integer lattice sums and finite-field combinations of codewords