Nested Lattice Codes Which Are Cyclic Groups

Chengpin Luo and Brian M. Kurkoski

Japan Advanced Institute of Science and Technology

Information Theory and Its Applications (ITA) Workshop
San Diego, California, USA
February 19, 2024

Motivation

Lattices have potential application to various communication systems

- Shaping gain using sphere-like constellation rather than QAM
- Compute-forward relay; particularly as a type of multiple access scheme
- Physical-layer network coding such as bi-directional relay
- Integer-forcing MIMO

Finite-length lattices are needed to practically realize such systems

---

This talk is about lattice codes that form a cyclic group. Potential benefit:

- Simplified encoding, since there is a single generator
- Various lattice codes may have fractional number of bits per dimension, leading to encoding loss. Using cyclic lattice code may reduce this loss.
- They are interesting

This is a cyclic group, not a cyclic code.

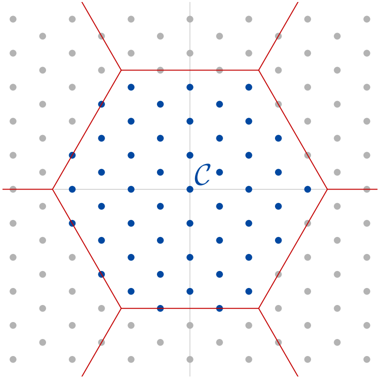
(Nested) Lattice Code

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
The generator matrix for Λ is $\mathbf{G}$:

$$\Lambda = \{\mathbf{G}\mathbf{b} \mid \mathbf{b} \in \mathbb{Z}^n\}$$

The check matrix is $\mathbf{H} = \mathbf{G}^{-1}$. A lattice code $\mathcal{C}$:

- $\mathcal{C}$ is the coset leaders of $\Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}}$
- Λ_{c} is the fine coding lattice with $\mathbf{G}_{\mathrm{c}}, \mathbf{H}_{\mathrm{c}}$
- Λ_{s} is the coarse shaping lattice with $\mathbf{G}_{\mathrm{s}}, \mathbf{H}_{\mathrm{s}}$
- Required to form lattice code:
  $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}} \Leftrightarrow \mathbf{H}_{\mathrm{c}}\mathbf{G}_{\mathrm{s}}$ is integer



A lattice is an infinite structure, a (nested) lattice code is a finite structure.

Self-Similar Lattice Codes.... Or Not?

Self-similar lattice code The shaping lattice Λ_{s} is scaled from the coding lattice Λ_{c}:

- $\mathcal{C} = \Lambda / M\Lambda$
- Sufficient for theoretical analysis (many results)

Non-self-similar lattice code[1] Practical reasons to not use self-similar lattices:

- Λ_{c} should have high coding gain and be easy to decode (e.g. lattices based on LDPC codes)
- Λ_{s} should have high shaping gain and have an efficient quantization algorithm:
    - Well-known lattices like E_8, Barnes-Wall, Leech, or
    - Convolutional code lattices with Viterbi algorithm quantization

[1] A more clever name is desired.

Rectangular Encoding

Rectangular encoding A bijective mapping from information $\mathbf{b}$ to codeword $\mathbf{x}$:

$$\begin{aligned}\mathbf{x} &= \mathbf{G}_\mathrm{c}\mathbf{b} - Q(\mathbf{G}_\mathrm{c}\mathbf{b}) \\ &= \mathbf{G}_\mathrm{c}\mathbf{b} \bmod \Lambda_\mathrm{s}\end{aligned}$$

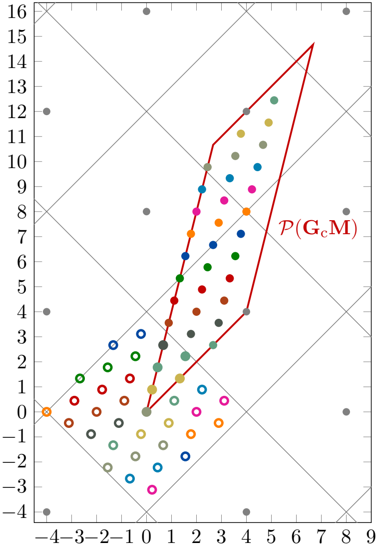
If the parallelogram $\mathcal{P}$ is a fundamental region for Λ_s:

- coding lattice inside $\mathcal{P}$ are coset leaders
- there is a one-to-one mapping between two cosets

Integers $\mathbf{b} = [b_1, b_2, \ldots, b_n]^\mathrm{t}$ are information:

$$b_i \in \{0, 1, \ldots, M_i - 1\}$$

$\mathcal{C}$ has $M = 2^{nR} = \prod_{i=1}^{n} M_i$ codewords



Cyclic Lattice Codes

A *cyclic group* is a group which can be generated by a single element $\mathbf{g}$, called the generator.

The integers $\mathbb{Z}$ are a cyclic group generated by 1 or -1 since $1+1=2$, $1+1+1=3$, etc.

A *cyclic lattice code*[2] is a nested lattice code which forms a cyclic group.

- Any lattice code $\Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}}$ is a group (see next slide)
- But in general, a lattice code is not a cyclic group

Self-similar lattice codes do not form a cyclic group. But under certain conditions, non-self-similar lattice codes do form a cyclic group.

[2] a cyclic group, not a cyclic code

Group Structure of Lattice Codes

A lattice code $\mathcal{C}$ forms a group under addition modulo Λ_s:

$$\mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{x}_1 + \mathbf{x}_2 \bmod \Lambda_\mathrm{s}$$

This group property is important for compute-forward.

A lattice code is generally not a cyclic group since $\mathbf{g}_1, \ldots, \mathbf{g}_n$ are linearly independent:

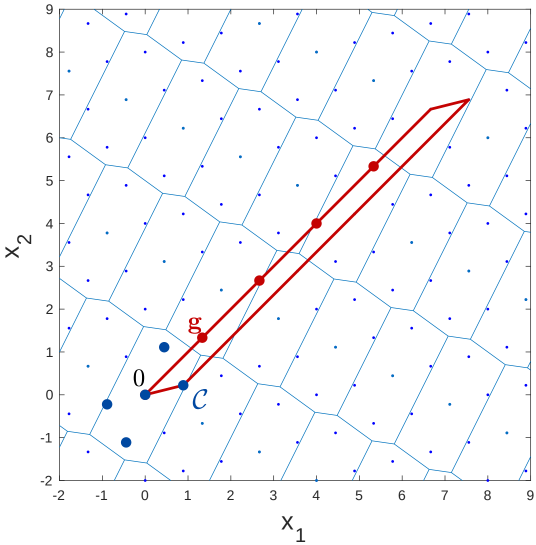
$$\mathbf{x} = \begin{bmatrix} | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \\ | & | & & | \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \bmod \Lambda_\mathrm{s}$$

But if we can find $[M_1, M_2, \ldots, M_n] = [1, 1, \ldots, M]$, then:

- b_1 to $b_{n-1} = 0$ and $\mathbf{g}_1$ to $\mathbf{g}_{n-1}$ are not used.
- $M_n = M$ and any codeword is given by $\mathbf{g}_n b_n \bmod \Lambda_\mathrm{s}$.
  The generator for the cyclic lattice code is $\mathbf{g}_n$.

How A Lattice Code Can Be Made Cyclic

- There is a one-to-one mapping between coset leaders in the parallelogram and $\mathcal{C}$.
- If all points in the parallelogram are generated by a single $\mathbf{g}$, then this will generate the whole group.
- Thus, $\mathcal{C}$ is cyclicly generated by $\mathbf{g}$.



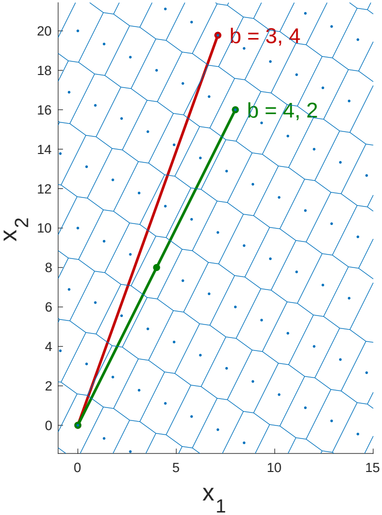
Technical Lemma

Lemma 1: Consider an n-dimension lattice Λ with generator matrix

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \dots & \mathbf{g}_n \end{bmatrix}$$

The line segment with endpoints $\mathbf{0}$ and $\mathbf{y} = \mathbf{G} \cdot \mathbf{b}$ with $\mathbf{b} = \begin{bmatrix} b_1 & b_2 & \dots & b_n \end{bmatrix}^T$ does not intersect any other point of Λ if and only if $\gcd(b_1, b_2, \dots, b_n) = 1$.

- $\mathbf{b} = [3, 4]$ are relatively prime — no other lattice point on the red segment
- $\mathbf{b} = [4, 2]$ 4 divides 2 — there is another lattice point on the green segment



Existence of Cyclic Lattice Codes

For the coding lattice Λ_{c},

$$\mathbf{G}_{\mathrm{c}} = \begin{bmatrix} | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \\ | & | & & | \end{bmatrix}$$

Define $\mathbf{q}_i$ as columns of:

$$\det(\mathbf{H}_{\mathrm{c}}\mathbf{G}_{\mathrm{s}})(\mathbf{H}_{\mathrm{c}}\mathbf{G}_{\mathrm{s}})^{-1} = \begin{bmatrix} | & | & & | \\ \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_n \\ | & | & & | \end{bmatrix}$$

Lemma 2: An n dimensional nested lattice code $\mathcal{C}$ with $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$ is a cyclic lattice code with generator $\mathbf{g}_i$ if and only if $\gcd(\mathbf{q}_i) = 1$.

This $\gcd$ condition is required only for column $\mathbf{q}_i$ corresponding to the cyclic generator $\mathbf{g}_i$.

Design for $n = 2$

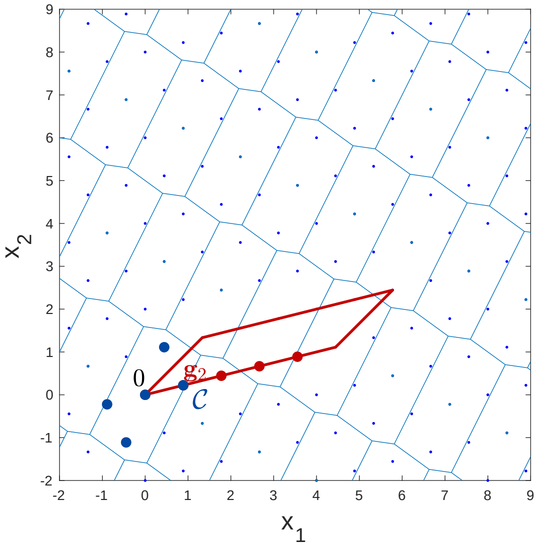
Consider coding lattice and shaping lattice with generator matrices:

$$\mathbf{G}_\mathrm{c} = \begin{bmatrix} \frac{4}{3} & \frac{8}{9} \\ \frac{4}{3} & \frac{2}{9} \end{bmatrix} \text{ and } \mathbf{G}_\mathrm{s} = \begin{bmatrix} \frac{16}{9} & \frac{4}{9} \\ \frac{22}{9} & \frac{28}{9} \end{bmatrix}$$

Then:

$$\det(\mathbf{H}_\mathrm{c}\mathbf{G}_\mathrm{s})(\mathbf{H}_\mathrm{c}\mathbf{G}_\mathrm{s})^{-1} = \begin{bmatrix} -4 & -3 \\ 1 & 2 \end{bmatrix}$$

- $4, 1$ are coprime, so $\mathbf{g}_1 = [\frac{4}{3}, \frac{4}{3}]^\mathrm{t}$ cyclicly generates $\mathcal{C}$
- $3, 2$ are coprime, so $\mathbf{g}_2 = [\frac{8}{9}, \frac{2}{9}]^\mathrm{t}$ cyclicly generates $\mathcal{C}$, also.



Possible Design for General n

Since the design places a restriction on $\mathbf{W}^{-1} = (\mathbf{H}_\mathrm{c}\mathbf{G}_\mathrm{s})^{-1}$, define $\mathbf{W}$ in a convenient form:

$$\mathbf{W} = \begin{bmatrix} 0 & \dots & 0 & a & b & c \\ 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 1 & 1 \\ w_{n,1} & \dots & w_{n,n-3} & w_{n,n-2} & w_{n,n-1} & w_{n,n} \end{bmatrix}.$$

For this design, $\gcd(c-b, a) = 1$ gives a cyclic lattice code, with matrix inversion using cofactors.

Group Isomorphism

Compute-and-forward requires the lattice code satisfy a group isomorphism:

$$\mathsf{enc}(\mathbf{b}_1 \boxplus \mathbf{b}_2) = \mathsf{enc}(\mathbf{b}_1) \oplus \mathsf{enc}(\mathbf{b}_2),$$

Feng, Silva and Kschischang gave conditions on the generator matrix to possess group isomorphism:

Lemma For arbitrary nested lattice $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$, if all elements from row i of $\mathbf{H}_{\mathrm{c}}\mathbf{G}_{\mathrm{s}}$ are divisible by M_i for all $i = 1, 2, ..., n$, then an isomorphism exists between group $\mathbf{b}, \boxplus$ and $\mathcal{C}, \oplus$.

To design a cyclic lattice code with group isomorphism Write the last row of $\mathbf{W}$:

$$\begin{bmatrix} r_1 M & r_2 M & \cdots & r_n M \end{bmatrix}$$

Then $\det(\mathbf{W}) = M$ leads to a linear diophantine equation in r_i.

Design Using $n = 8$ with E_8 for Shaping

Suppose we want to design a (1) cyclic lattice code with $M = 64$ codewords (rate 0.75) which has (2) shaping gain provided by the E_8 lattice and possesses (3) group isomorphism.

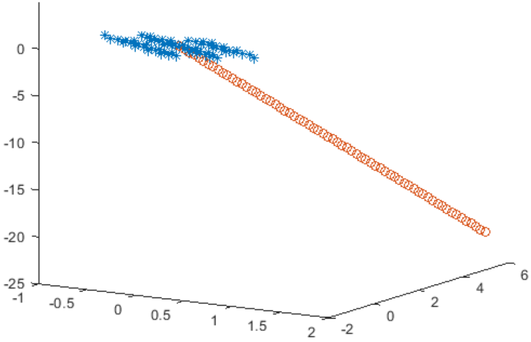
$$\mathbf{W} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & a & b & c \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & Mr_6 & Mr_7 & Mr_8 \end{bmatrix}.$$

Choose $(a, b, c) = (7, 17, 19)$ to make the lattice cyclic. Solve $\det(\mathbf{W}) = 64$ to obtain $(r_6, r_7, r_8) = (95, 65, 92)$.

Finally, choose $\mathbf{G}_{\mathrm{c}} = \mathbf{G}_{\mathrm{s}}\mathbf{W}^{-1}$. This gives a coding lattice with coding gain 2.67 dB

Design Using $n = 8$ with E_8 for Shaping

As a consequence of having three "design" columns in $\mathbf{W}$, the resulting lattice code is in 3 dimensions



Conclusion

- Gave conditions under which a lattice code forms a cyclic group.
- Gave a few basic constructions with dimension $n = 2$ and $n = 8$.
- Possibly simplifies encoding by replacing a generator matrix with a generator vector
- May reduce mapping overhead when the number of bits/dimension is not a power of two.