Voronoi Constellations for High-dimensional Lattice Codes

Nuwan Ferdinand*, **Matthew Nokleby#** and Behnaam Aazhang¤

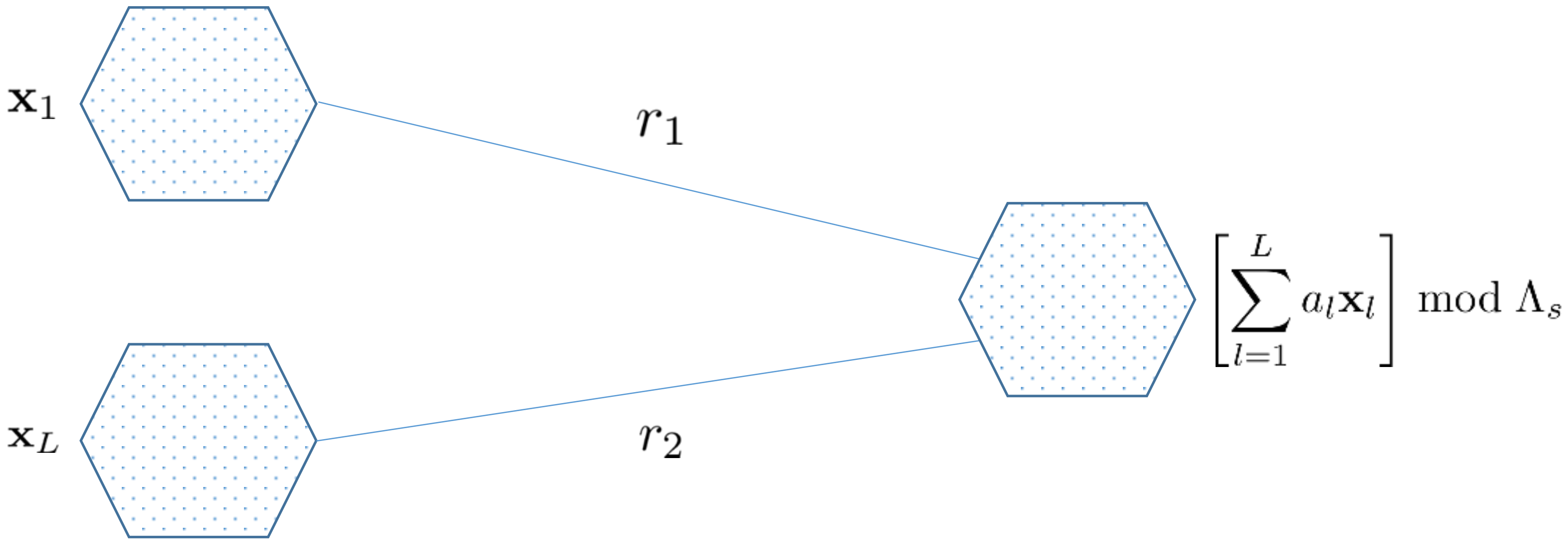
University of Toronto, Toronoto, ON, Cananda*

Wayne State University, Detroit, MI, USA#

Rice University, TX, USA¤

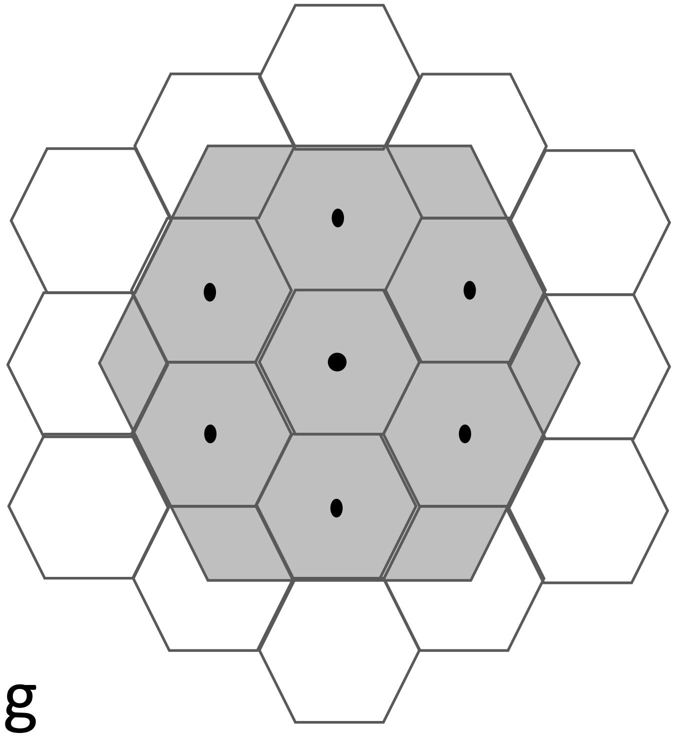
Why lattice codes?

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



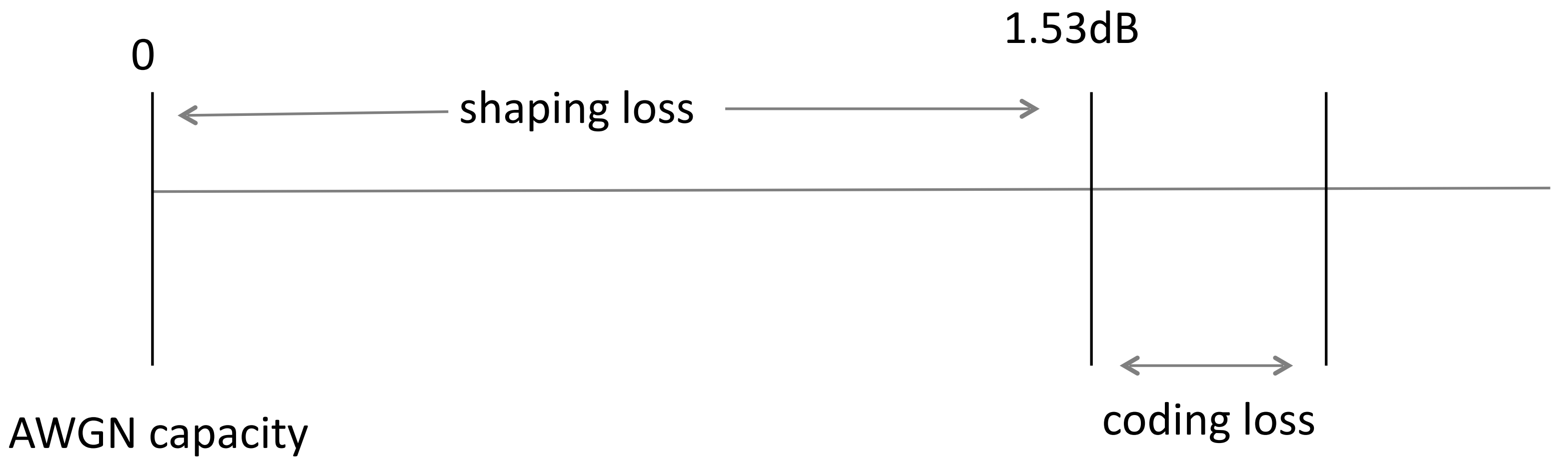
Lattice codes in theory

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

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

Lattice definitions

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

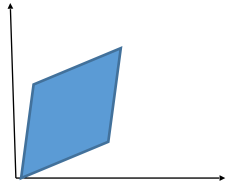
$$\mathcal{Q}_{\Lambda_n}(\mathbf{x}) = \arg\max_{\lambda \in \Lambda_n} \|\mathbf{x} - \lambda\|$$

- The modulo-lattice operation with respect to Λ_n returns the quantization error:

$$\mathbf{x} \bmod \Lambda_n = \mathbf{x} - \mathcal{Q}_{\Lambda_n}(\mathbf{x})$$

Lattice definitions

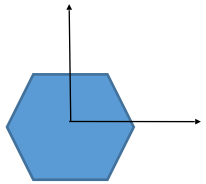
- Let $\mathcal{P}_n$ denote the fundamental parallelepiped region of Λ_n with respect to a generator G:



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

- There is a shifted parallelepiped region for each point of Λ_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 Λ_n is the set of points that are closer to $\lambda = \mathbf{0}$ lattice point than to any other lattice point.



Coding lattice structure

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_{11} & 0 & 0 & 0 & 0 & 0 \\ \mathbf{G}_{21} & \mathbf{G}_{22} & 0 & 0 & 0 & 0 \\ \mathbf{G}_{31} & \mathbf{G}_{32} & \mathbf{G}_{33} & 0 & 0 & 0 \\ . & . & . & . & 0 & 0 \\ . & . & . & . & . & 0 \\ \mathbf{G}_{(n/m)1} & . & . & . & & \mathbf{G}_{(n/m)(n/m)} \end{bmatrix}$$

- Break lattice into blocks of length m, m<<n
- Lower-triangular generator matrix
- $G_{ij} = g_r I_m$ 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:

$$\mathbf{b} \in \mathbb{Z}^n$$

$$\mathbf{b} = [(\mathbf{b}^1)^T, (\mathbf{b}^2)^T, \ldots (\mathbf{b}^{n/m})^T]^T$$

$$\mathbf{b}^r = (b_1^r, \ldots, b_m^r)^T$$

$$b_i^r \in \{0, 1, \ldots, g_r^{-1}\theta_{ii} - 1\}$$

- 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

$$\mathbf{b}^r \in \mathbb{Z}^m \leftrightarrow \mathbf{c}^r \in g_r^{-1}\mathcal{P}_m \cap \mathbb{Z}^m$$

$$\mathbf{f}^r = \left(\frac{b_i^r}{g_r^{-1}\theta_{11}} \;\; \frac{b_2^r}{g_r^{-1}\theta_{22}} \;\; \cdots \frac{b_m^r}{g_r^{-1}\theta_{mm}} \right)^T$$

$$\mathbf{f}^r \in [0,1)^m$$

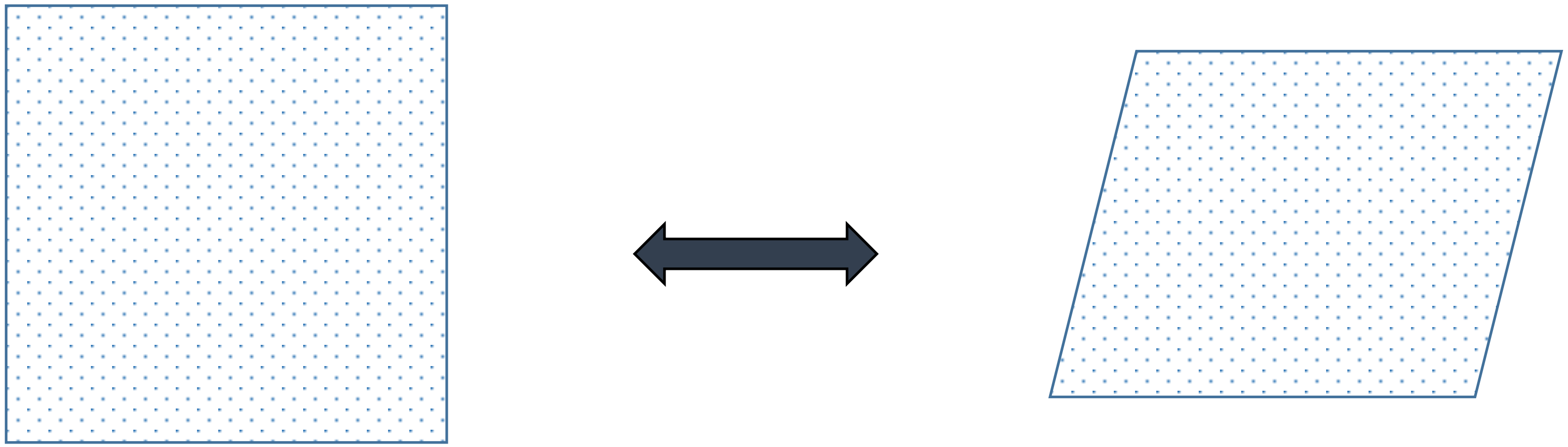
$$\mathbf{c}^r = g_r^{-1}\Theta\mathbf{f}^r$$

$$\mathbf{c} = [(\mathbf{c}^1)^T \;\; (\mathbf{c}^2)^T \ldots (\mathbf{c}^{n/m})^T]^T$$

Code construction-encoding

$$\mathbf{b}^r \in \mathbb{Z}^m \leftrightarrow \mathbf{c}^r \in g_r^{-1}\mathcal{P}_m \cap \mathbb{Z}^m$$

$$b_i^r \in \{0, 1, \ldots, g_r^{-1}\theta_{ii} - 1\}$$



$\mathbf{b}^r \in \mathbb{Z}^m$

$\mathbf{c}^r \in g_r^{-1}\mathcal{P}_m \cap \mathbb{Z}^m$

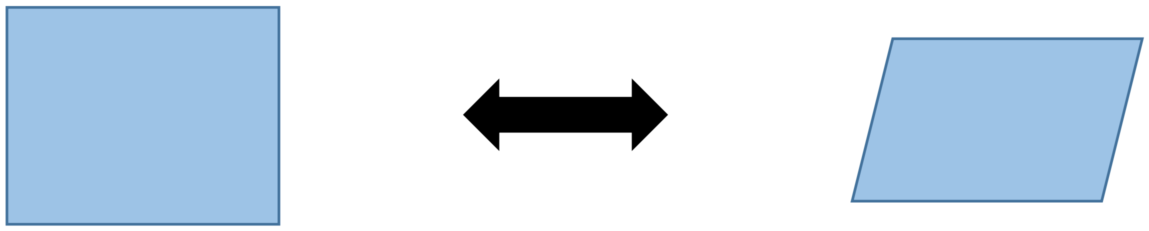
Code construction-encoding

- We introduce a subtractive dither:

$$\mathbf{a}^r = [0,1)^m$$

$$\mathbf{d}^r = \Theta\mathbf{a}^r$$

$$\mathbf{d} = [(\mathbf{d}^1)^T\ (\mathbf{d}^2)^T \ldots (\mathbf{d}^{n/m})^T]^T$$



$\mathbf{a}^r$:

$\mathbf{d}^r = \Theta\mathbf{a}^r$

Code construction-encoding

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

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

$$\mathbf{x}' = \mathbf{G}(\mathbf{c} - \bar{\mathbf{G}}^{-1}\mathbf{d} - \mathbf{q})$$

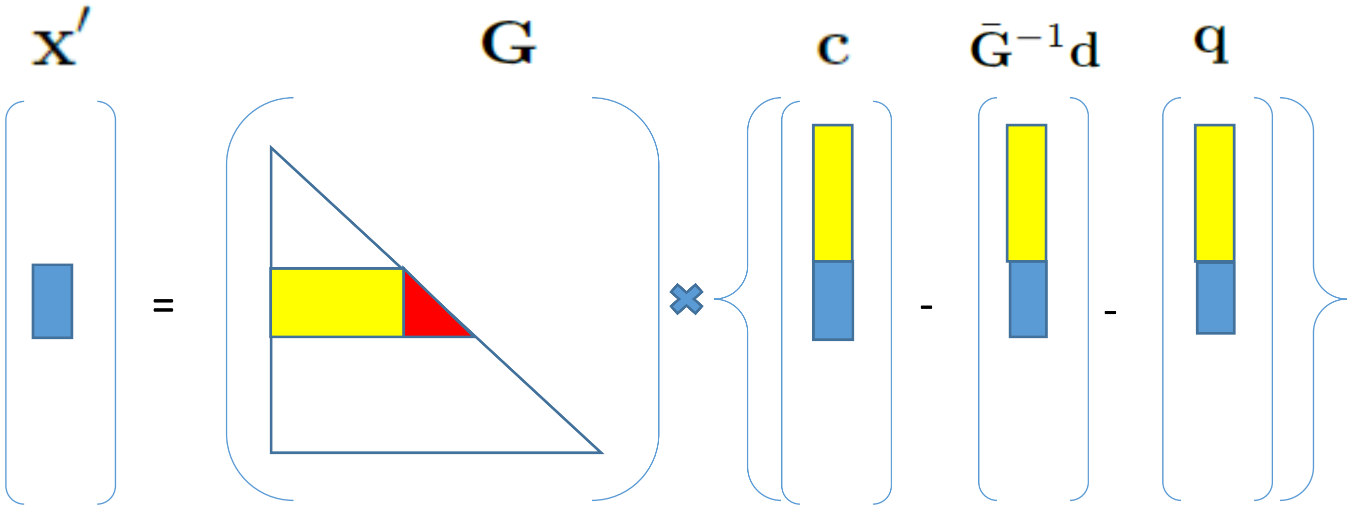
Code construction-encoding

$$\mathbf{q}^r = [q_{((r-1)m+1)} \cdots q_{(rm)}]^T \in \mathbb{Z}^m$$

$$\mathbf{x}'^r = [x'_{(r-1)m+1} \ldots x'_{rm}]^T \in \mathbb{R}^m$$

$$\mathbf{c}^r = [c_{(r-1)m+1} \ldots c_{rm}]^T \in \mathbb{Z}^m$$

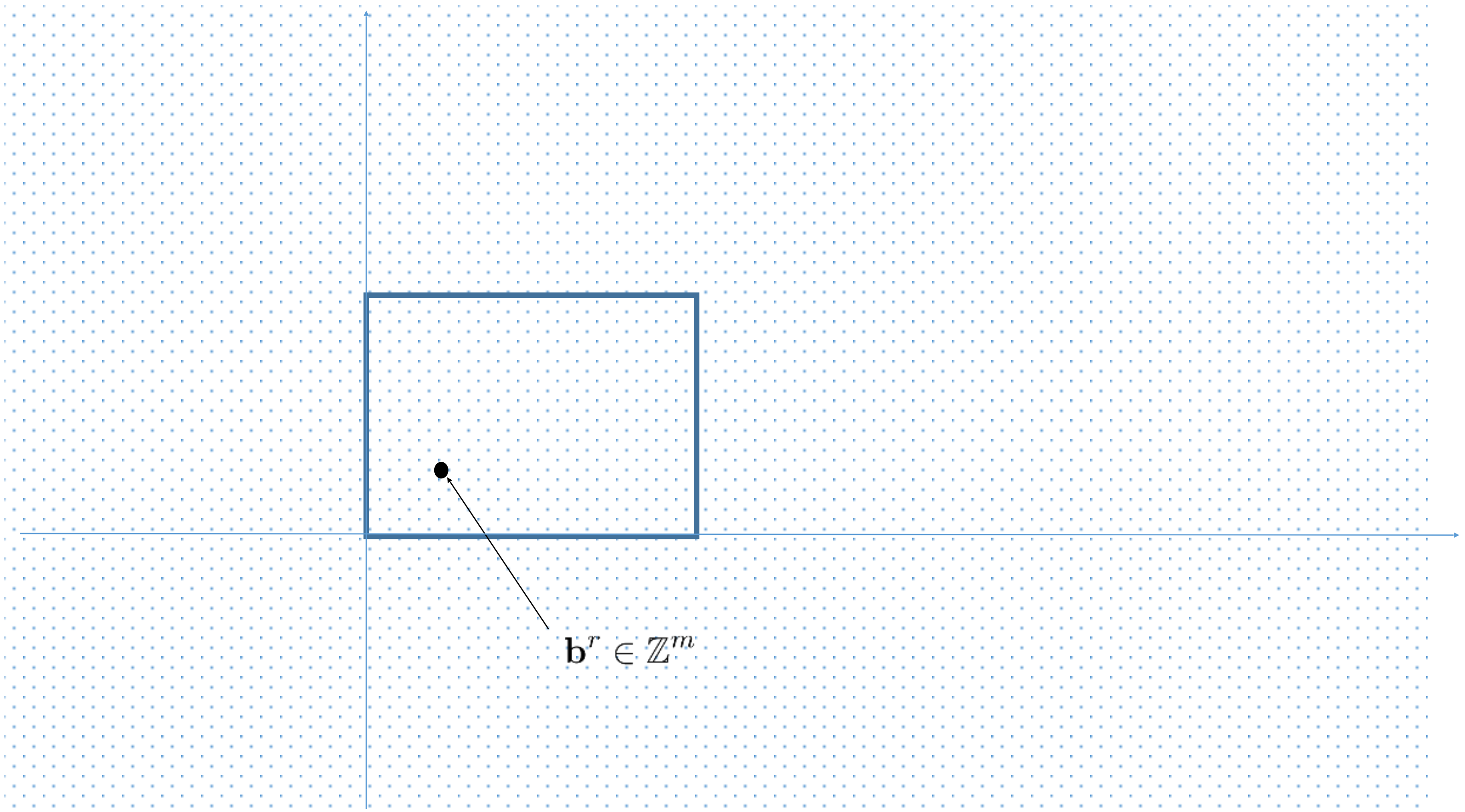
$$\mathbf{d}^r = [d_{(r-1)m+1} \ldots d_{rm}]^T \in \mathcal{P}_m$$



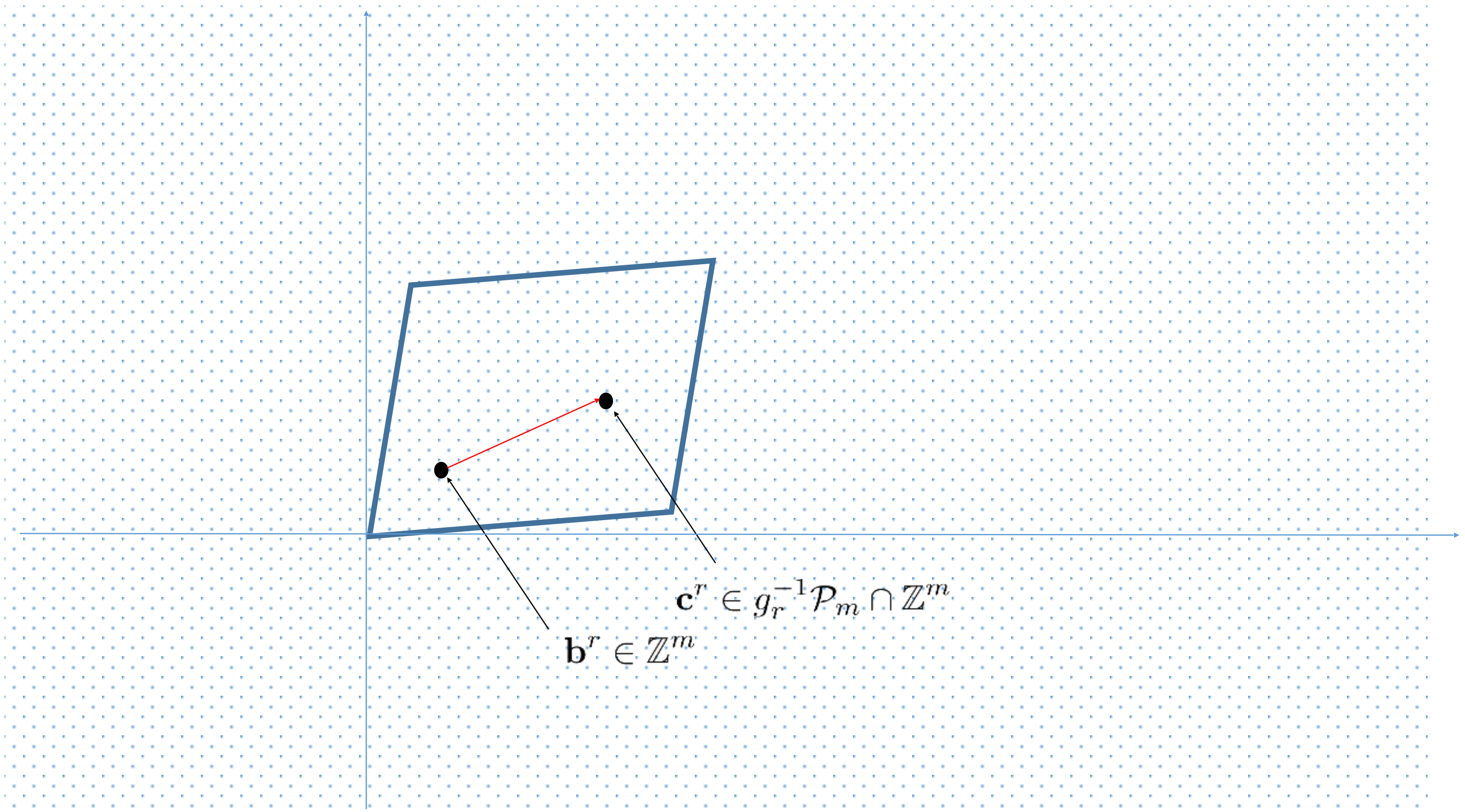
$\mathbf{s}^r = [\mathbf{G}_{r1}\mathbf{G}_{r2} \ldots \mathbf{G}_{r(r-1)}] \cdot [(\mathbf{k}^1)^T(\mathbf{k}^2)^T \ldots (\mathbf{k}^{r-1})^T]^T$ where $\mathbf{k}^r = \mathbf{c}^r - g_r^{-1}\mathbf{d}^r - \mathbf{q}^r$

$$\begin{aligned}\mathbf{x}'^r &= \mathbf{G}_{rr}(\mathbf{c}^r - g_r^{-1}\mathbf{d}^r - \mathbf{q}^r) + \mathbf{s}^r \\ &= g_r\mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r - g_r\mathbf{q}^r.\end{aligned}$$

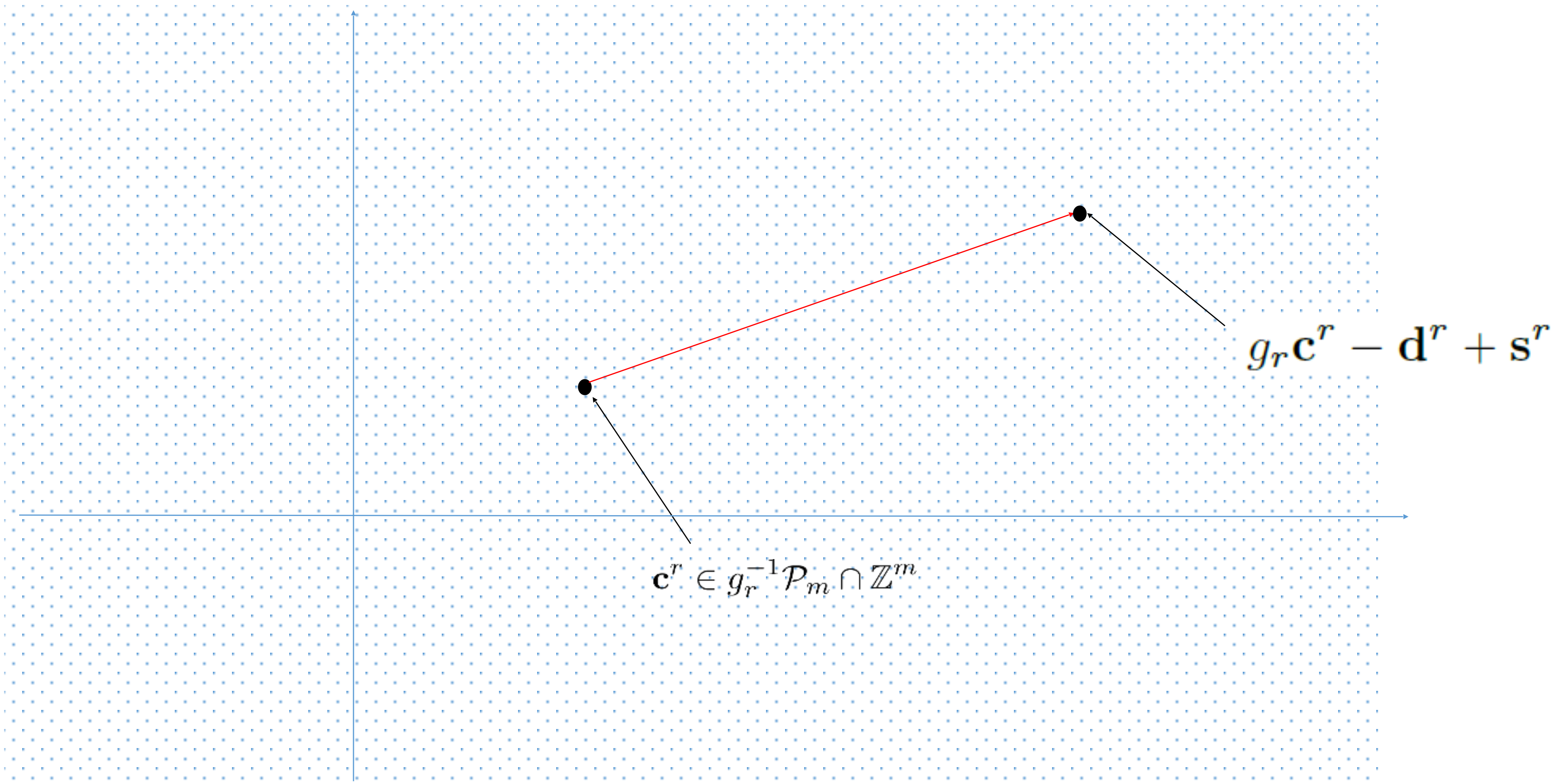
Code construction-encoding



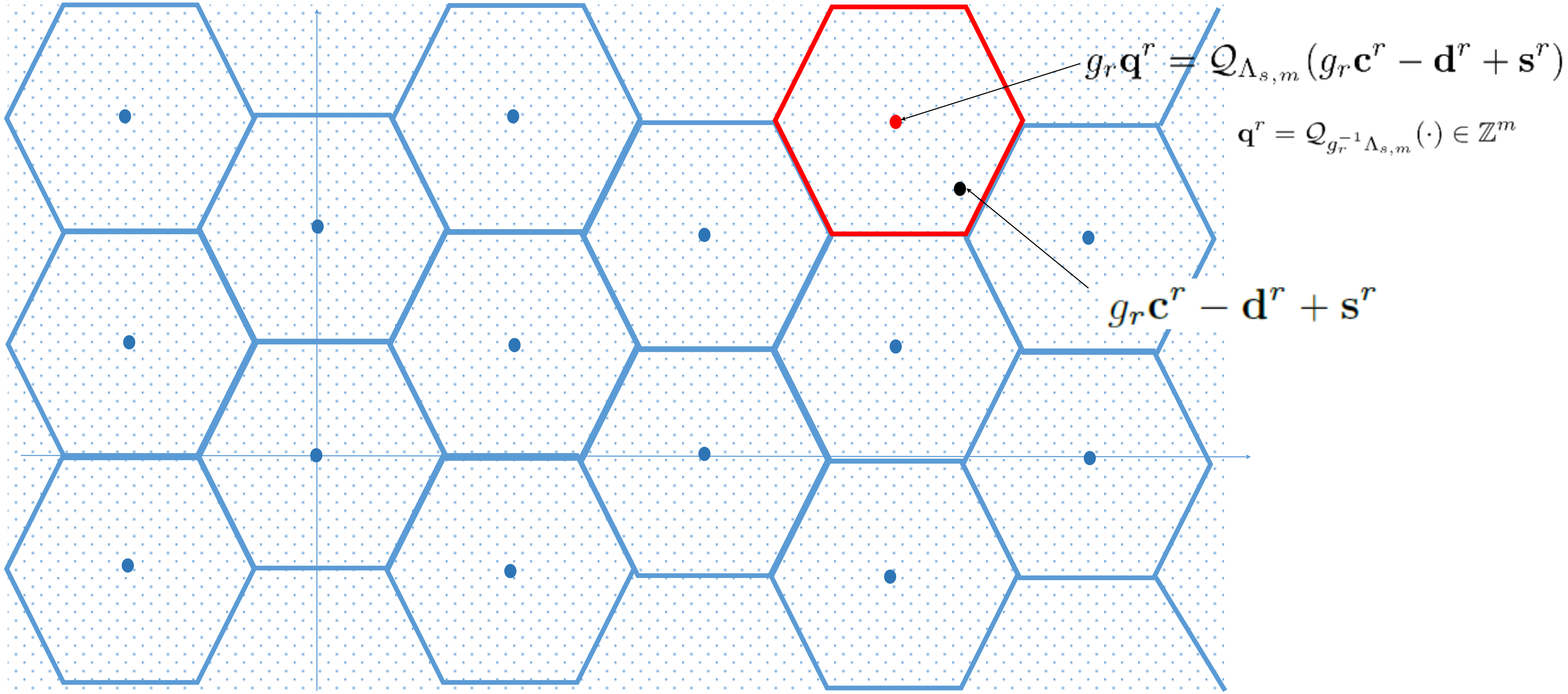
Code construction-encoding



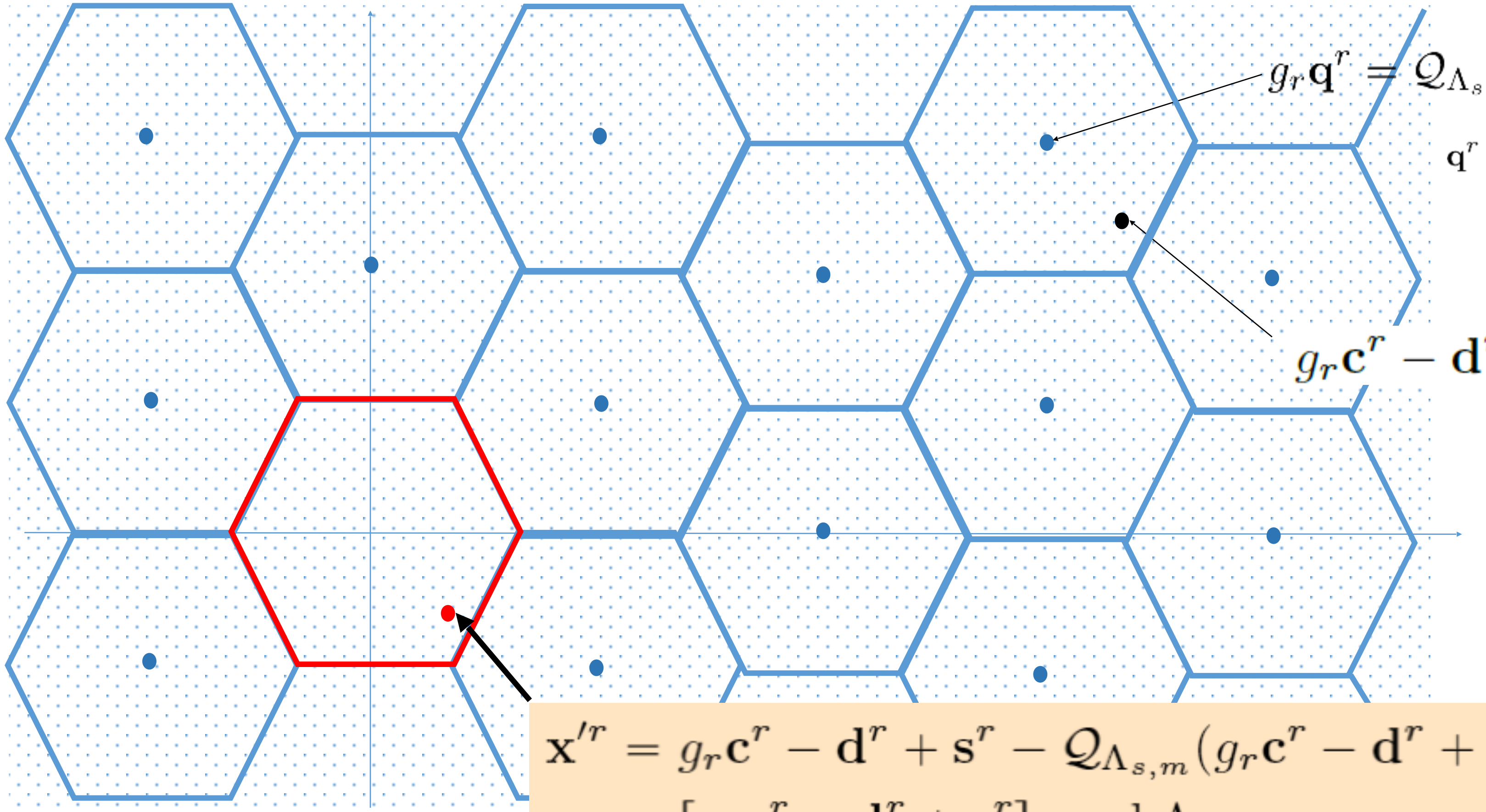
Code construction-encoding



Code construction-encoding



Code construction-encoding



$$\begin{aligned}\mathbf{x}'^r &= g_r\mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r - \mathcal{Q}_{\Lambda_{s,m}}(g_r\mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r)\\ &= [g_r\mathbf{c}^r - \mathbf{d}^r + \mathbf{s}^r] \bmod \Lambda_{s,m}.\end{aligned}$$

Decoding

$$\mathbf{y} = h\mathbf{x}' + \mathbf{z},$$

$$\hat{\mathbf{x}} = \mathcal{Q}_{\Lambda_{c,n}}\left(h^{-1}\mathbf{y} + \mathbf{G}\bar{\mathbf{G}}^{-1}\mathbf{d}\right)$$

$$\mathbf{w} = \mathbf{c} - \mathbf{q}$$

$$\mathbf{w}^r = \mathbf{c}^r - \mathbf{q}^r$$

$$\mathbf{w}^r = g_r^{-1}\Theta\mathbf{f}^r - \mathbf{q}^r$$

$$\mathbf{w}^r = g_r^{-1}\Theta\mathbf{f}^r - g_r^{-1}\Theta\bar{\mathbf{q}}^r \qquad \mathbf{q}^r \in g_r^{-1}\Lambda_{s,m} \qquad \bar{\mathbf{q}}^r \in \mathbb{Z}^m$$

$$g_r\Theta^{-1}\mathbf{w}^r = \mathbf{f}^r - \bar{\mathbf{q}}^r$$

$$\mathbf{f}^r = [g_r\Theta^{-1}\mathbf{w}^r] \bmod \mathbb{Z}^m \qquad \mathbf{f}^r \in [0,1)^m$$

$$\mathbf{b}^r = g_r^{-1}\bar{\Theta}[g_r\Theta^{-1}\mathbf{w}^r] \bmod \mathbb{Z}^m$$

Complexity

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

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

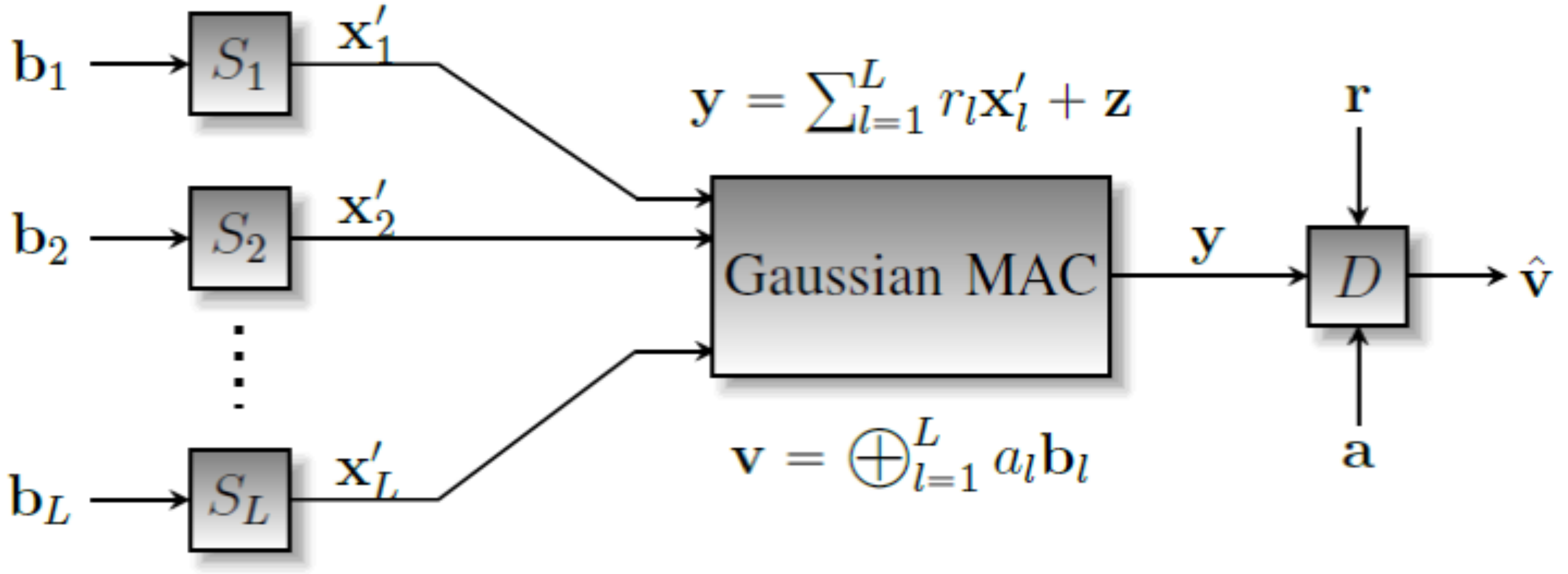
Where n – dimensional of coding lattice
c – complexity involved in quantization step using shaping lattice. For E8 lattice c=72.
m – dimensional of shaping lattice. For E8 lattice m=8.
d – number of non-zero elements in generator matrix of coding lattice. For LDLC, LDA, d=8.

Performance

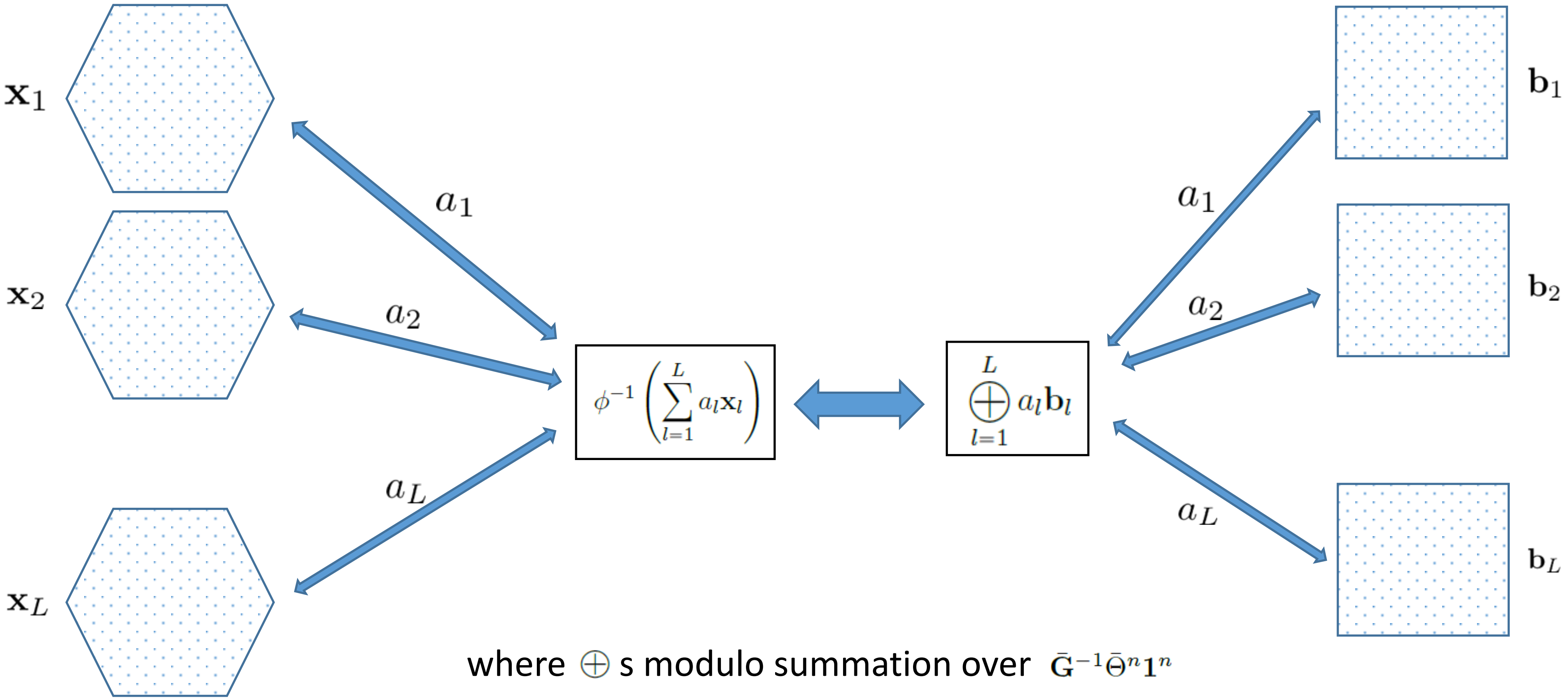
- **Theorem:** The shaping loss of the full shaping lattice is the same as the shaping loss of $\Lambda_{s,m}$
  Proof: Taking Cartesian products does not affect the normalized second moment of a lattice.
- Can exploit the shaping properties of E8, BW16 lattices

- **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



Mapping for compute and forward



$\Lambda_{c,n} \cap \mathcal{V}_{s,n}$

where $\oplus$ s modulo summation over $\bar{\mathbf{G}}^{-1}\bar{\Theta}^n \mathbf{1}^n$

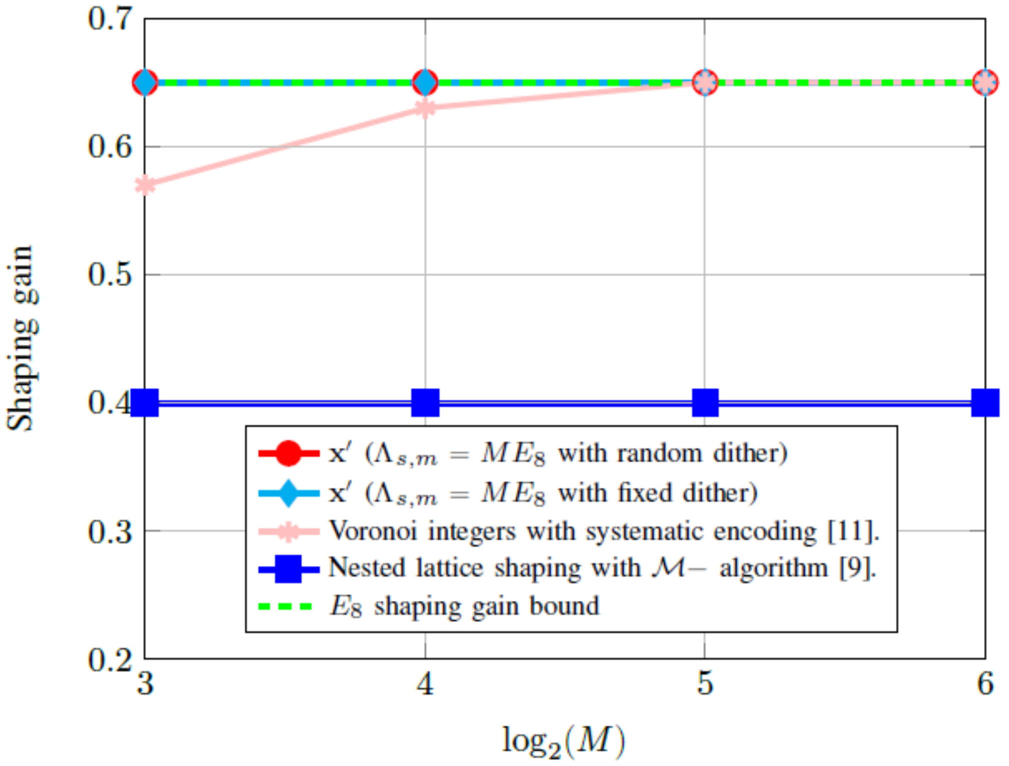
$$\phi^{-1}(\mathbf{u}) = \bar{\mathbf{G}}^{-1}\bar{\Theta}^n \left([\bar{\mathbf{G}}(\Theta^n)^{-1}\mathbf{G}^{-1}\mathbf{u}] \bmod \mathbb{Z}^n \right)$$

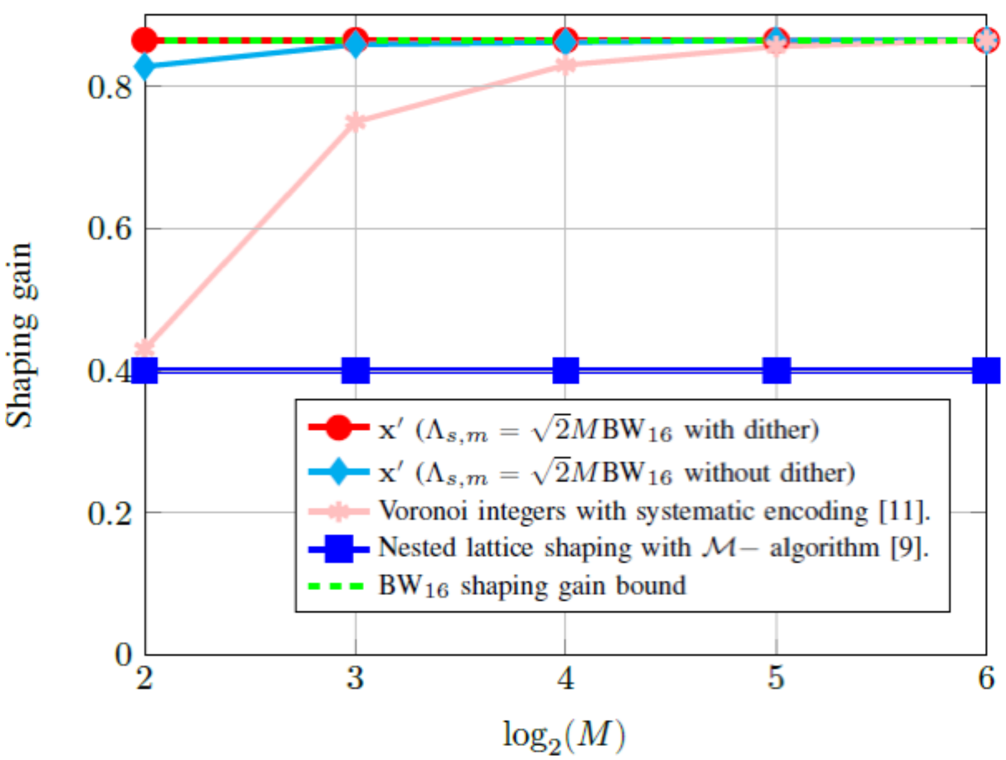
$$\Theta^n = \begin{bmatrix} \Theta & & & \\ & \Theta & & \\ & & \ddots & \\ & & & \Theta \end{bmatrix}$$

Which finite field?

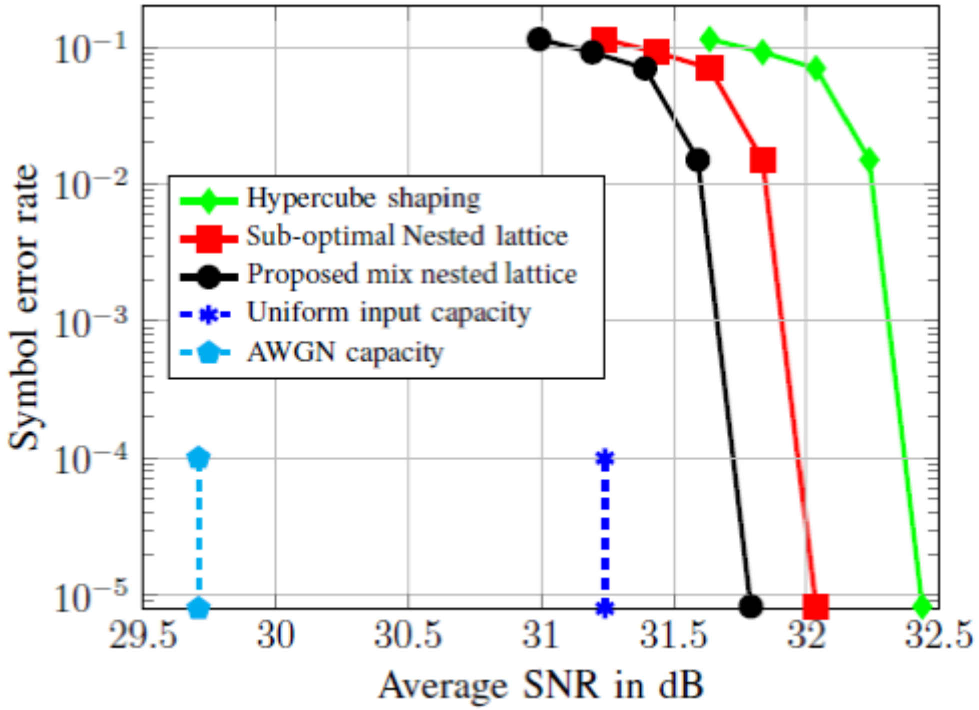
- Compute-and-forward requires modulo summation over a prime field
- This requirement can be satisfied by designing shaping matrices such that $g_{ii}^{-1}\theta_{ii} = p^{l_i}$ where p is a prime number and $l_i \in \mathbb{Z}$
- For lattices such as scaled D_m, E_8 and BW_{16}, the related prime number is $p = 2$
- Can experimentally design lattices for higher primes

Shaping gain-numerical results





Symbol error performance: with LDLC as coding lattice.



Symbol error rate versus average SNR for Voronoi integers. For $n = 10^4$ and $\mathcal{R} = 4.935$ 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