Construction π_A Lattices: A Review and Recent Results

Yu-Chih (Jerry) Huang

Department of Communication Engineering
National Taipei University

Joint work with Krishna Narayanan @ Texas A&M University

Lattice codes are everywhere

(Nested) Lattice codes have many applications in IT

- See paper "Lattices are Everywhere" by Zamir
- Single user Gaussian channel - Erez & Zamir
- Coding with side information (Wyner-Ziv and Costa) - Zamir, Erez & Shamai
- Physical layer network coding - Wilson et al, Nam et al
- Secrecy - He & Yener, Ling et al
- Interference alignment - Sridharan, Jafaraian, Vishwanath & Jafar and Ordentlich, Erez, & Nazer
- Dirty multiple access channel - Philosof, Khisti, Erez & Zamir
- Compute-and-forward - Nazer & Gastpar

Most of these results are based on Construction A lattices

Lattice codes are everywhere

(Nested) Lattice codes have many applications in IT

- See paper "Lattices are Everywhere" by Zamir
- Single user Gaussian channel - Erez & Zamir
- Coding with side information (Wyner-Ziv and Costa) - Zamir, Erez & Shamai
- Physical layer network coding - Wilson et al, Nam et al
- Secrecy - He & Yener, Ling et al
- Interference alignment - Sridharan, Jafaraian, Vishwanath & Jafar and Ordentlich, Erez, & Nazer
- Dirty multiple access channel - Philosof, Khisti, Erez & Zamir
- Compute-and-forward - Nazer & Gastpar

Most of these results are based on Construction A lattices

Generate asymptotically good lattices; but comes with large decoding complexity

Lattice codes are everywhere

(Nested) Lattice codes have many applications in IT

- See paper "Lattices are Everywhere" by Zamir
- Single user Gaussian channel - Erez & Zamir
- Coding with side information (Wyner-Ziv and Costa) - Zamir, Erez & Shamai
- Physical layer network coding - Wilson et al, Nam et al
- Secrecy - He & Yener, Ling et al
- Interference alignment - Sridharan, Jafaraian, Vishwanath & Jafar and Ordentlich, Erez, & Nazer
- Dirty multiple access channel - Philosof, Khisti, Erez & Zamir
- Compute-and-forward - Nazer & Gastpar

Most of these results are based on Construction A lattices

Generate asymptotically good lattices; but comes with large decoding complexity

Main theme: Construction that generates good lattices with low complexity

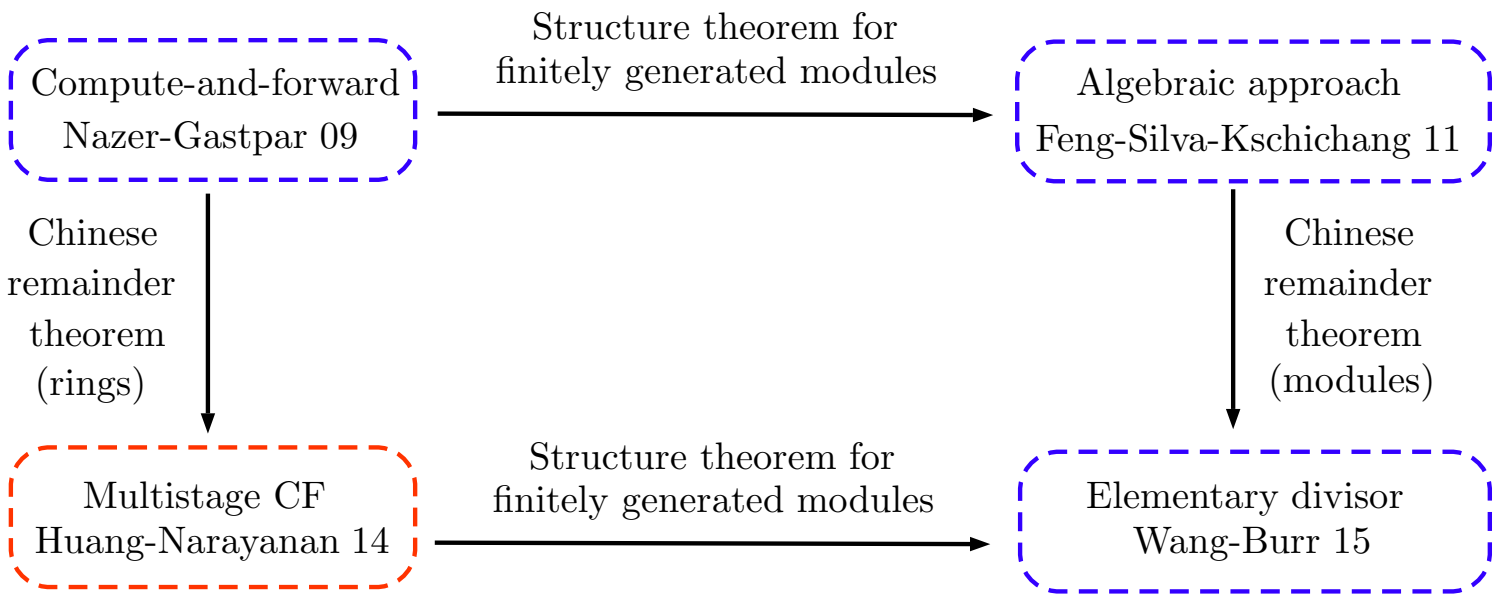
My view of these constructions

After Alister's talk on Monday, I was like

My view of these constructions

After Alister's talk on Monday, I was like

My view of these constructions



Construction π_A is special case of EDC where we can show interesting things

Lattices

n-dimensional lattice Λ^n: A discrete subgroup of $\mathbb{R}^n$

- Can be expressed by generator matrix $\mathbf{G}$ as

$$\Lambda^n = \{\mathbf{Gz} : \mathbf{z} \in \mathbb{Z}^n\}$$

- Closed under
  - Addition: $\lambda_1, \lambda_2 \in \Lambda^n$ implies $\lambda_1 + \lambda_2 \in \Lambda^n$
  - Reflection: $\lambda_1 \in \Lambda^n$ implies $-\lambda_1 \in \Lambda^n$

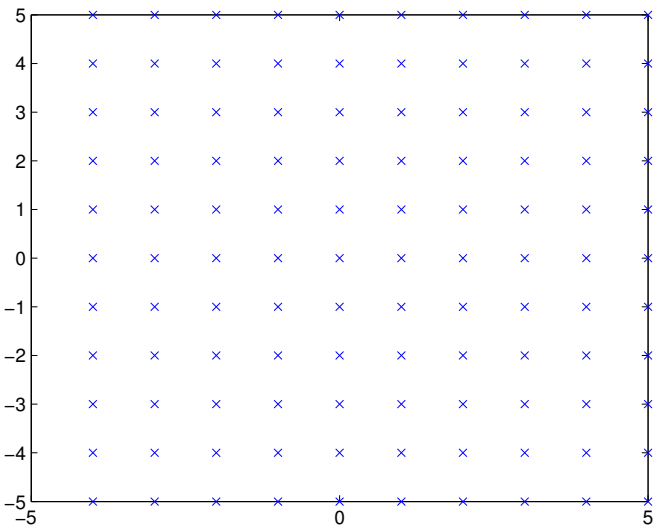


Figure: Rectangular (Z_2) lattice, Gaussian integers $\mathbb{Z}[i]$

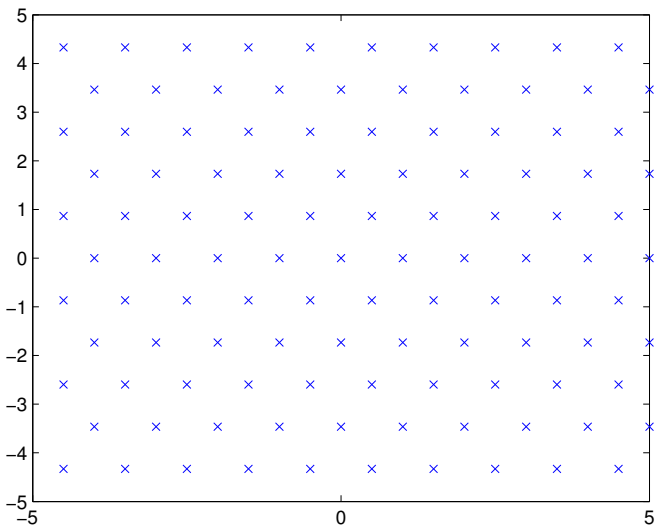
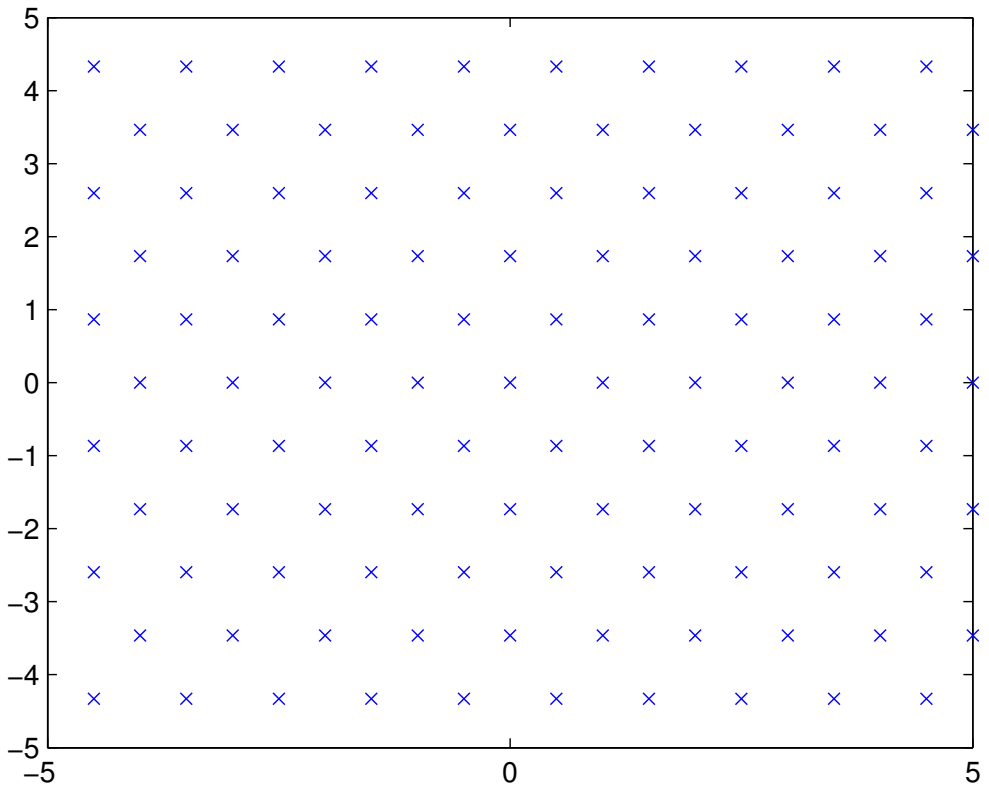


Figure: Hexagonal (A_2) lattice, Eisenstein integers $\mathbb{Z}[\omega]$

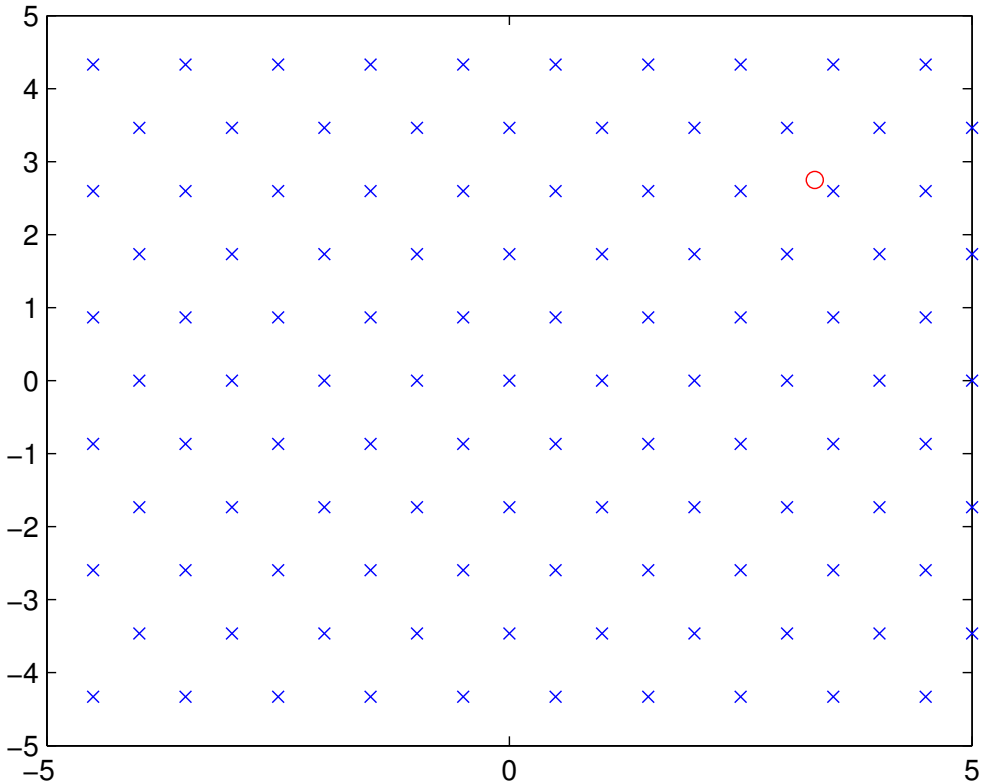
Lattices

- Lattice quantizer: For $\mathbf{x} \in \mathbb{R}^n$, $Q_\Lambda(\mathbf{x}) \triangleq \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|^2$
- Fundamental Voronoi region: $\mathcal{V}(\Lambda) \triangleq \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = 0\}$
- Modulo operation: For $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \mod \Lambda \triangleq \mathbf{x} - Q_\Lambda(\mathbf{x})$



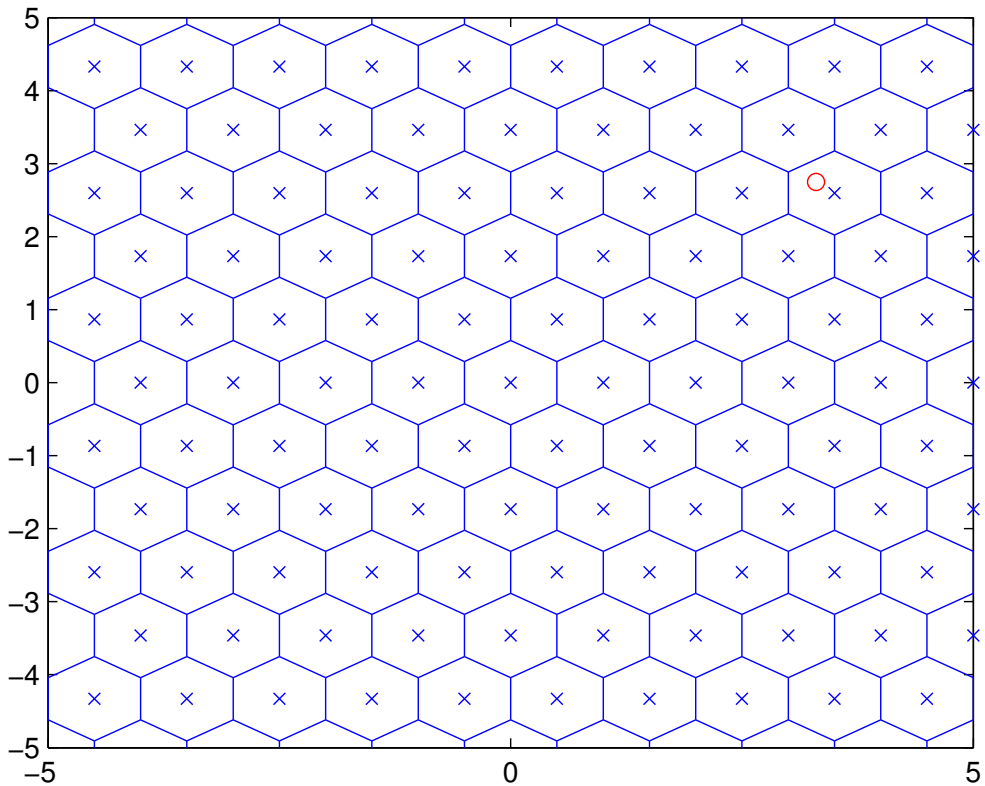
Lattices

- Lattice quantizer: For $\mathbf{x} \in \mathbb{R}^n$, $Q_\Lambda(\mathbf{x}) \triangleq \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|^2$
- Fundamental Voronoi region: $\mathcal{V}(\Lambda) \triangleq \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = 0\}$
- Modulo operation: For $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \mod \Lambda \triangleq \mathbf{x} - Q_\Lambda(\mathbf{x})$



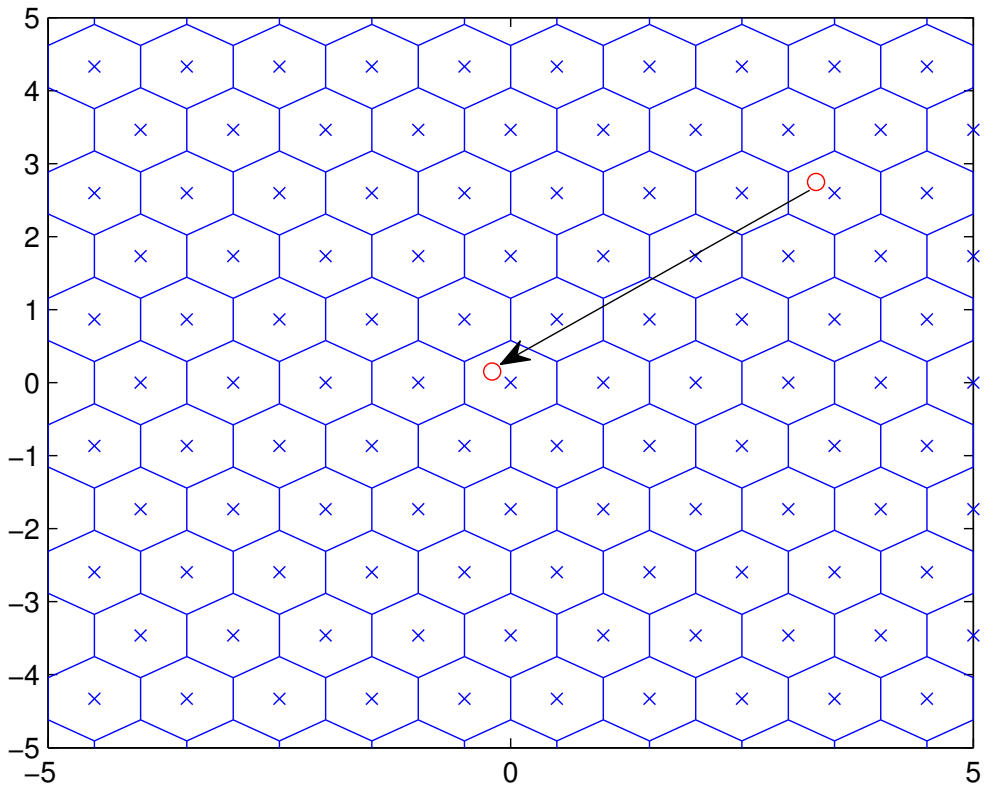
Lattices

- Lattice quantizer: For $\mathbf{x} \in \mathbb{R}^n$, $Q_\Lambda(\mathbf{x}) \triangleq \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|^2$
- Fundamental Voronoi region: $\mathcal{V}(\Lambda) \triangleq \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = 0\}$
- Modulo operation: For $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \mod \Lambda \triangleq \mathbf{x} - Q_\Lambda(\mathbf{x})$



Lattices

- Lattice quantizer: For $\mathbf{x} \in \mathbb{R}^n$, $Q_\Lambda(\mathbf{x}) \triangleq \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|^2$
- Fundamental Voronoi region: $\mathcal{V}(\Lambda) \triangleq \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = 0\}$
- Modulo operation: For $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \mod \Lambda \triangleq \mathbf{x} - Q_\Lambda(\mathbf{x})$



Goodness for MSE quantization

- Let $\mathbf{U} \sim$Uniform$(\mathcal{V})$
- Second moment per dim associated with Λ

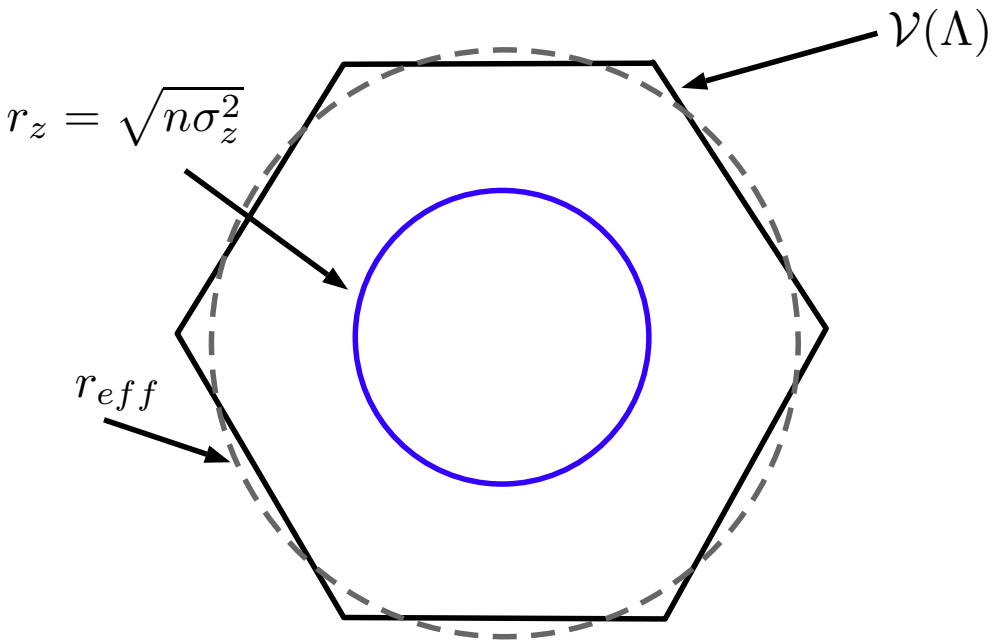
$$\sigma^2(\Lambda) \triangleq \frac{1}{n}\mathbb{E}\|\mathbf{U}\|^2 = \frac{1}{n}\frac{\int_{\mathcal{V}} \|\mathbf{x}\|^2 d\mathbf{x}}{\mathsf{Vol}(\Lambda)}$$

- Normalized second moment (NSM) of Λ

$$G(\Lambda) \triangleq \frac{\sigma^2(\Lambda)}{\mathsf{Vol}(\Lambda)^{\frac{2}{n}}} > \frac{1}{2\pi e}$$

- Note that $r\mathcal{B}$ has $G(r\mathcal{B}) \to 1/(2\pi e)$
- A seq of Λ^n is good for MSE quantization if has $G(\Lambda) \to 1/(2\pi e)$
- Related to performance of lattice quantizer at high resolution

Goodness for channel coding



- Consider using Λ as our transmitted constellation, no power constraint, over AWGN channel

$$\mathbf{y} = \boldsymbol{\lambda} + \mathbf{z}, \quad \mathbf{z} \sim N(\mathbf{0}, \sigma_z^2 \mathbf{I})$$

- Use lattice decoding, i.e., decoding to $Q_\Lambda(\mathbf{y})$
- From LLN, $\mathbf{z}$ lies inside $r_z \mathcal{B}$ w.h.p.
- A seq of lattices is good for channel coding if $p_e \to 0$ whenever $r_{eff} > r_z$

Outline

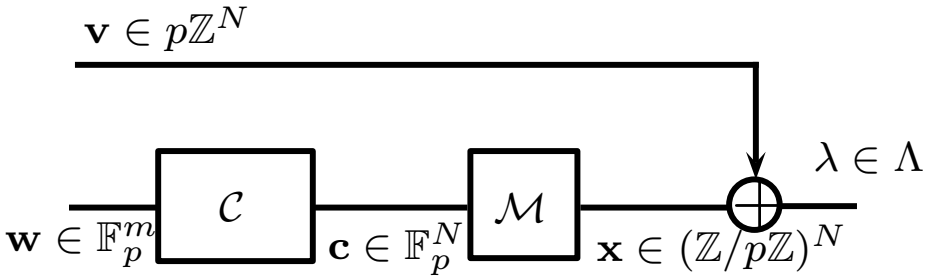
1. Construction A Lattices Review
2. Construction π_A Multilevel Lattices
3. Application 1: Multistage Compute-and-Forward
4. Application 2: Lattice Index Coding
5. Future Directions

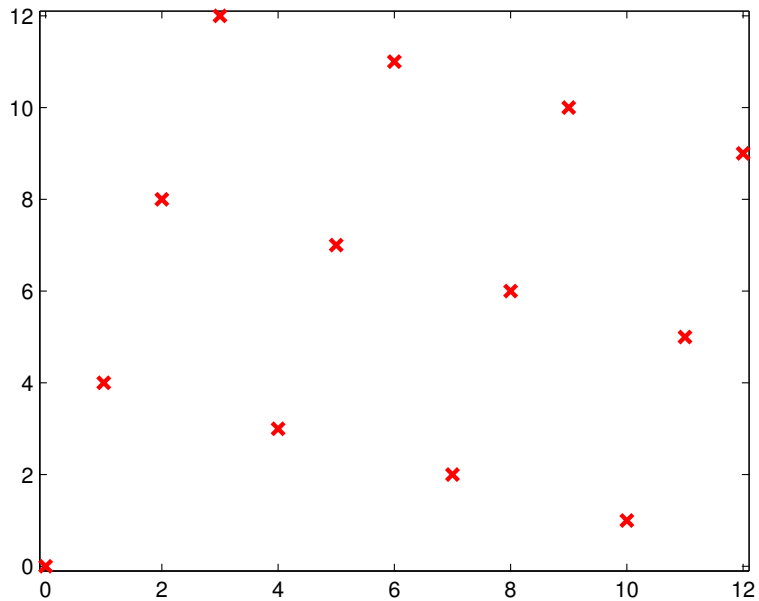
Outline

1. Construction A Lattices Review
2. Construction π_A Multilevel Lattices
3. Application 1: Multistage Compute-and-Forward
4. Application 2: Lattice Index Coding
5. Future Directions

N-Dim Lattice Using Construction A (Leech-Sloane 71)

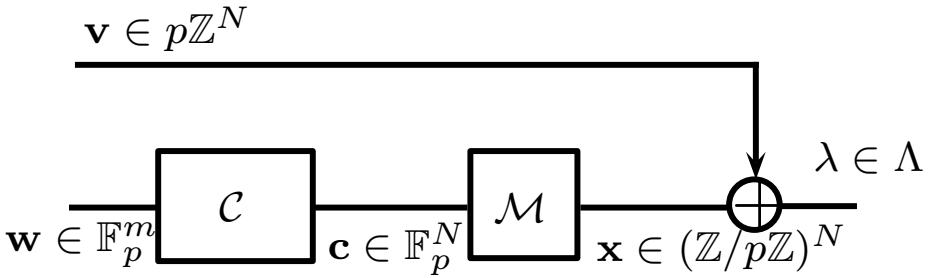
- C linear code over $\mathbb{F}_p$
- $\mathcal{M} : \mathbb{F}_p \to \mathbb{Z}$ natural mapping
- $\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

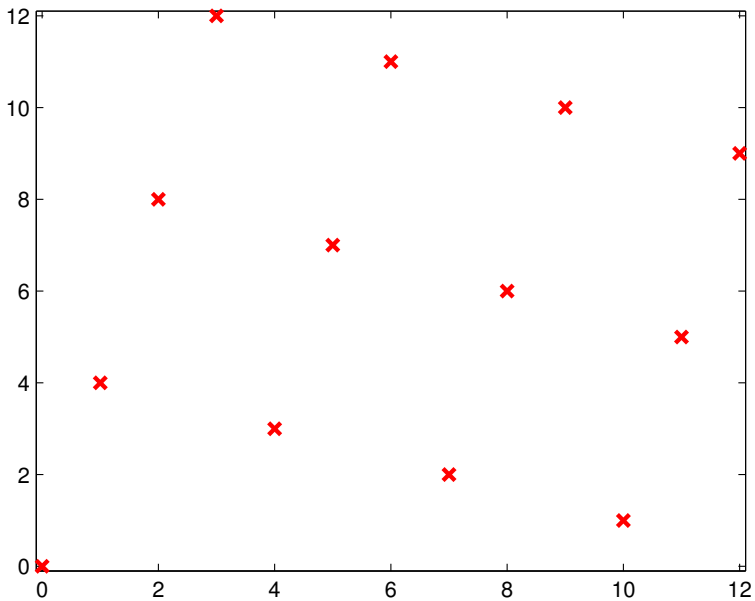


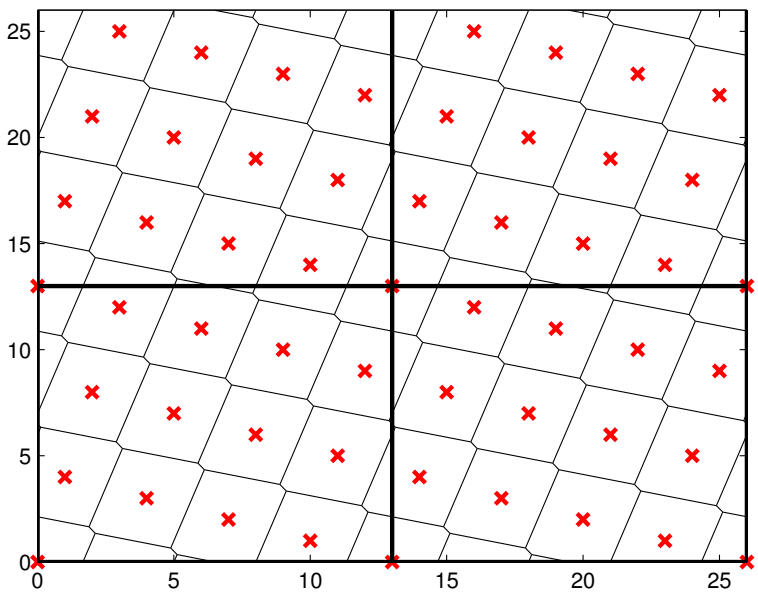


N-Dim Lattice Using Construction A (Leech-Sloane 71)

- C linear code over $\mathbb{F}_p$
- $\mathcal{M} : \mathbb{F}_p \to \mathbb{Z}$ natural mapping
- $\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$
- $\lambda \in \Lambda$ iff $\lambda \bmod p\mathbb{Z}^N \in C$



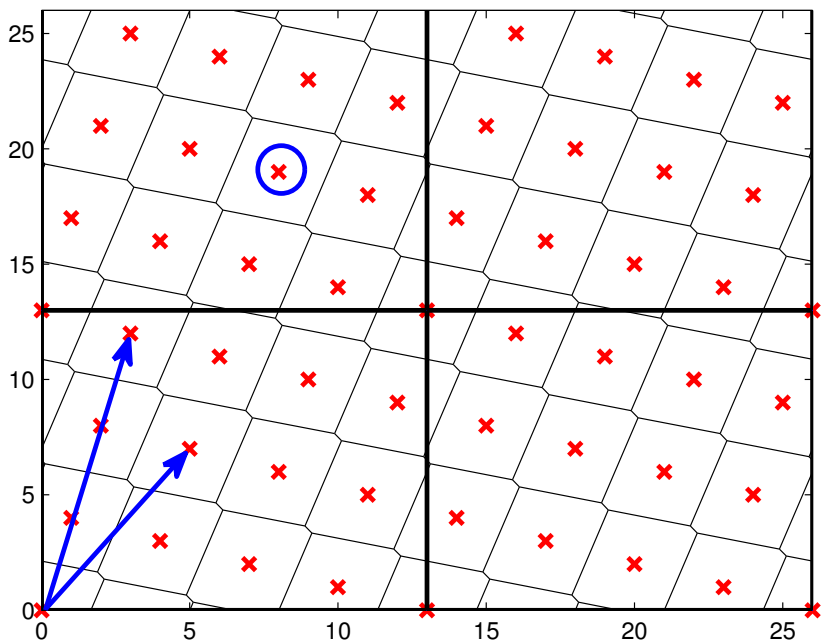




Construction A: What makes this a Lattice?

Construction A: $\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

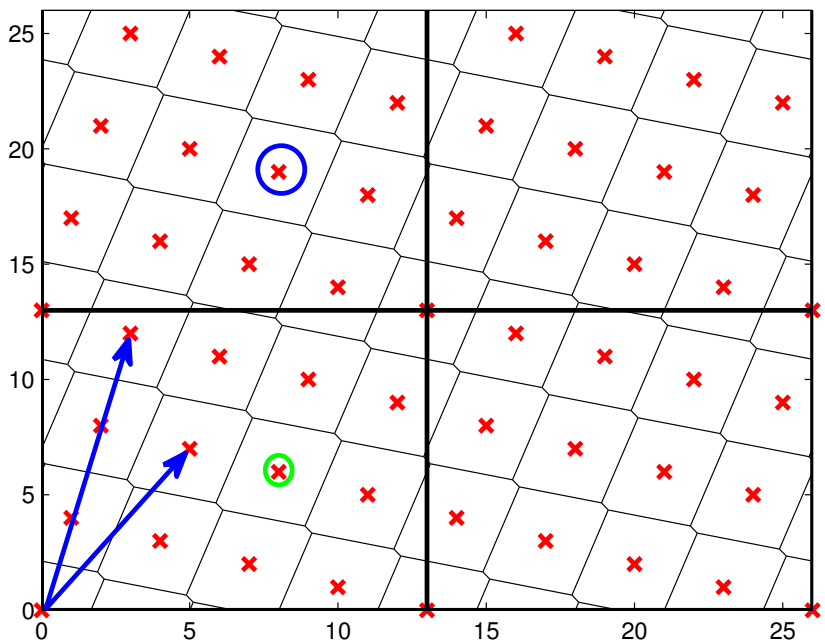
- $\boldsymbol{\lambda}_1 = \mathcal{M}(\mathbf{c}_1) + p\mathbf{k}_1$ and $\boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_2$
- $\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_1) + \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_1 + p\mathbf{k}_2$
- It becomes $\mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2) + p\mathbf{k}_3$
- Thus, $(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)$ mod $p\mathbb{Z}^N = \mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2)$



Construction A: What makes this a Lattice?

Construction A: $\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

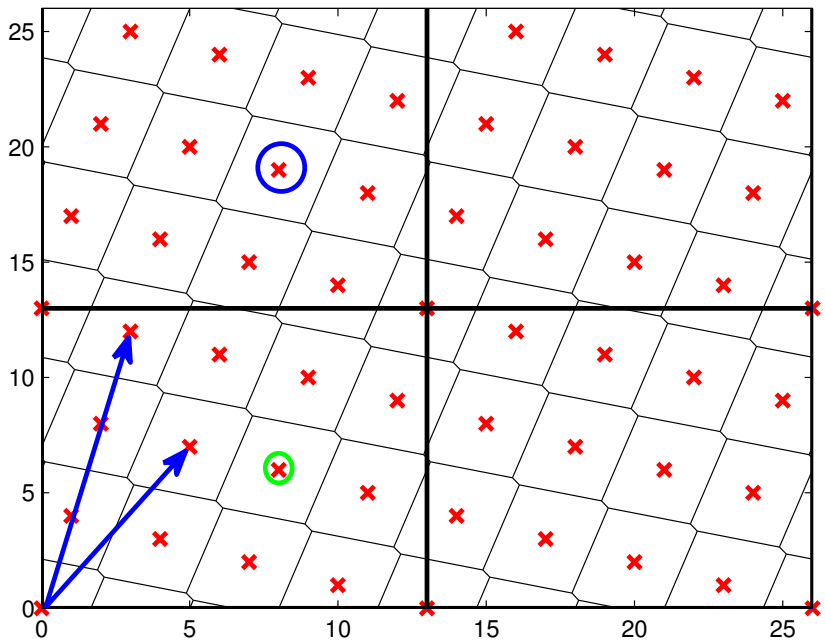
- $\boldsymbol{\lambda}_1 = \mathcal{M}(\mathbf{c}_1) + p\mathbf{k}_1$ and $\boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_2$
- $\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_1) + \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_1 + p\mathbf{k}_2$
- It becomes $\mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2) + p\mathbf{k}_3$
- Thus, $(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)$ mod $p\mathbb{Z}^N = \mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2)$



Construction A: What makes this a Lattice?

Construction A: $\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

- $\boldsymbol{\lambda}_1 = \mathcal{M}(\mathbf{c}_1) + p\mathbf{k}_1$ and $\boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_2$
- $\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 = \mathcal{M}(\mathbf{c}_1) + \mathcal{M}(\mathbf{c}_2) + p\mathbf{k}_1 + p\mathbf{k}_2$
- It becomes $\mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2) + p\mathbf{k}_3$
- Thus, $(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2)$ mod $p\mathbb{Z}^N = \mathcal{M}(\mathbf{c}_1 \oplus \mathbf{c}_2)$



Natural mapping and mod p preserve ring structures between $\mathbb{Z}$ and $\mathbb{F}_p$

Why Construction A with natural mapping would work?

$\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

- $\mathcal{M}^{-1}((\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) \bmod p\mathbb{Z}) = \mathbf{c}_1 \oplus \mathbf{c}_2$
- This would work if $\mathcal{M}^{-1} \circ \bmod p\mathbb{Z}$ is ring homomorphism

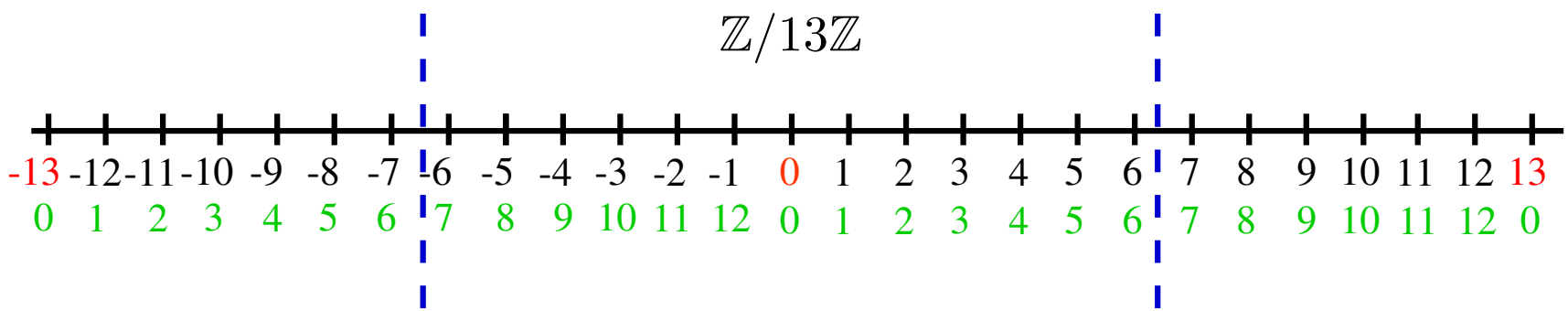
Why Construction A with natural mapping would work?

$\Lambda = \mathcal{M}(C) + p\mathbb{Z}^N$

- $\mathcal{M}^{-1}((\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) \bmod p\mathbb{Z}) = \mathbf{c}_1 \oplus \mathbf{c}_2$
- This would work if $\mathcal{M}^{-1} \circ \bmod p\mathbb{Z}$ is ring homomorphism

Quotient ring

- $p\mathbb{Z}$ is an ideal in $\mathbb{Z}$
- Coset decomposition $\mathbb{Z}/p\mathbb{Z}$ results in a quotient ring
- For prime p, $p\mathbb{Z}$ is maximal ideal (since $\mathbb{Z}$ is PID)
- $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$



Generalizations

Construction A over $\mathbb{Z}$: $\mathcal{M}$ natural mapping

- Natural mapping happens to be ring isomorphism
- $\mod p$ is canonical ring homomorphism
- $\varphi \triangleq \mathcal{M}^{-1} \circ \mod p$ is ring homo

Generalizations

Construction A over $\mathbb{Z}$: $\mathcal{M}$ natural mapping

- Natural mapping happens to be ring isomorphism
- $\mod p$ is canonical ring homomorphism
- $\varphi \triangleq \mathcal{M}^{-1} \circ \mod p$ is ring homo
- This is all the math I am going to use

Generalizations:

Generalizations

Construction A over $\mathbb{Z}$: $\mathcal{M}$ natural mapping

- Natural mapping happens to be ring isomorphism
- $\mod p$ is canonical ring homomorphism
- $\varphi \triangleq \mathcal{M}^{-1} \circ \mod p$ is ring homo
- This is all the math I am going to use

Generalizations:

- Construction A over $\mathbb{Z}[\omega]$
  - Increase average computation rates for compute-and-forward (CF)
  - Construction and application to CF: T-IT 15
- Go beyond PID, Construction A over $\mathfrak{O}_{\mathbb{K}}$
  - Consider only rings of imaginary quadratic integers
  - Propose adaptive CF where TX adaptively work with best $\mathfrak{O}_{\mathbb{K}}$
  - ISIT 15 and will be submitted to T-IT soon
- Construction π_A
  - Can be used to decrease decoding complexity
  - Naturally suited for broadcasting with receiver side information
  - ITW 13, ISIT 14, T-IT submitted 15, under revision 16

Outline

1 Construction A Lattices Review

2 Construction π_A Multilevel Lattices

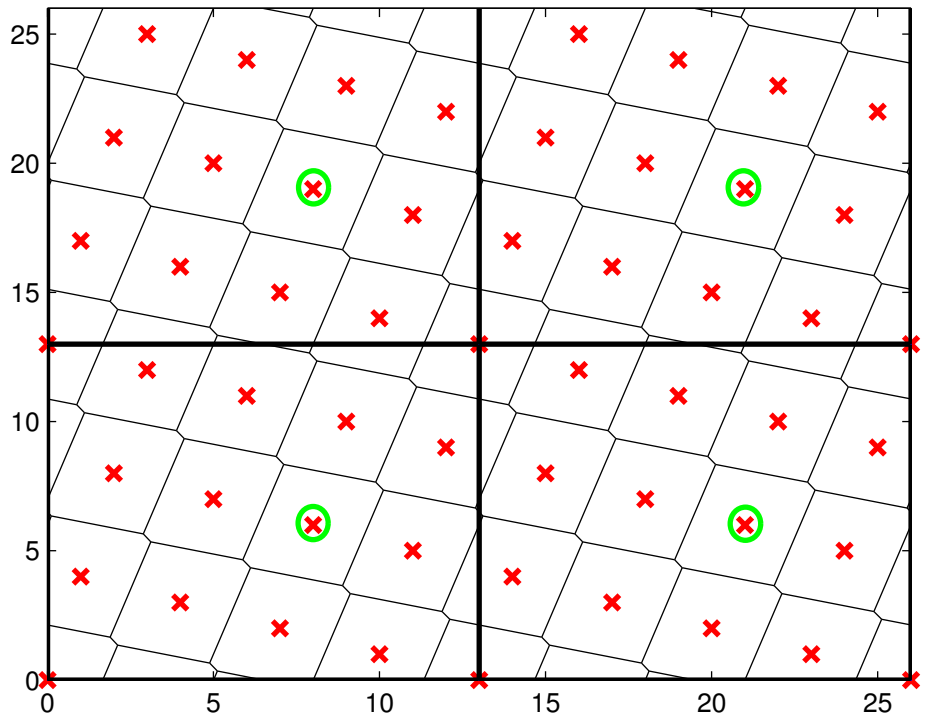
3 Application 1: Multistage Compute-and-Forward

4 Application 2: Lattice Index Coding

5 Future Directions

Motivation: Problem with Construction A

$$\lambda = \mathcal{M}(\mathbf{c}) + p \cdot \mathbf{k} \text{ where } \mathbf{c} \in C \text{ and } \mathbf{k} \in \mathbb{Z}^N$$



- $\mathbf{k}$ is unprotected; p has to be large to have a good lattice
- Complexity depends on decoding the linear code over $\mathbb{F}_p$
- E.g., simulation results by di Pietro, Boutros, Zemor, Brunel with $\mathbb{F}_{11}$ and $\mathbb{F}_{41}$

Main result in this part

Construction π_A based on the Chinese Remainder Theorem

- p does not have to be prime - can be replaced by $p_1 p_2 \dots p_L$
- Instead of working over $\mathbb{F}_p$, we can work over $\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \dots \times \mathbb{F}_{p_l}$
- Ex: $q = 210$ with just codes over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$
- Show existence of sequence of lattices that are optimal

In short: New construction of lattices that preserve algebraic structures and goodness with substantially lower complexity

Chinese Remainder Theorem for Commutative Rings

Let $p_1, \ldots, p_L$ be distinct primes, $q = p_1 \cdot p_2 \ldots p_L$, and $q_l = q/p_l$

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_L} \cong \mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \ldots \times \mathbb{F}_{p_L}$$

An isomorphism:

$$\mathcal{M}(v^1, \ldots, v^L) = s_1 q_1 v^1 + \ldots + s_L q_L v^L \mod q\mathbb{Z},$$

where $s_1, \ldots, s_L$ are sols to Bézout's identity $s_1 q_1 + \ldots + s_L q_L = 1$.

Example 1

Chinese Remainder Theorem for Commutative Rings

Let $p_1, \ldots, p_L$ be distinct primes, $q = p_1 \cdot p_2 \ldots p_L$, and $q_l = q/p_l$

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_L} \cong \mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \ldots \times \mathbb{F}_{p_L}$$

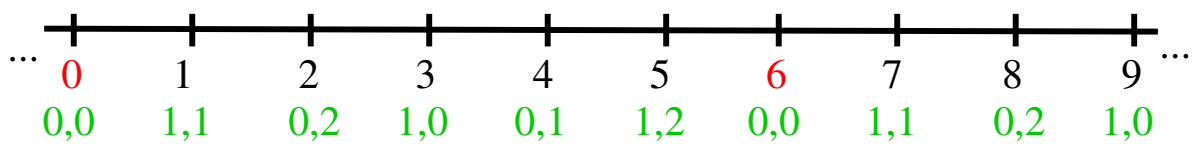
An isomorphism:

$$\mathcal{M}(v^1, \ldots, v^L) = s_1 q_1 v^1 + \ldots + s_L q_L v^L \mod q\mathbb{Z},$$

where $s_1, \ldots, s_L$ are sols to Bézout's identity $s_1 q_1 + \ldots + s_L q_L = 1$.

Example 1

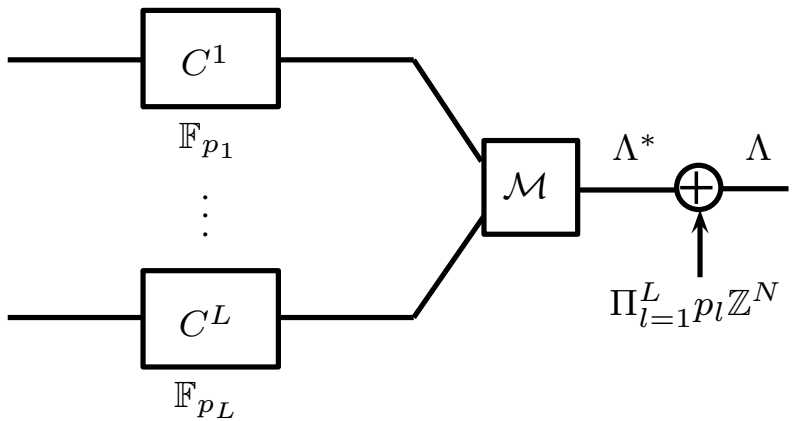
Consider $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$. An isomorphism: $\mathcal{M} = 3v^1 - 2v^2 \mod 6\mathbb{Z}$



Construction π_A (previously called product construction)

Let $p_1, \ldots, p_L$ be distinct primes and $q = p_1\ p_2 \ldots p_L$.

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_L}$$



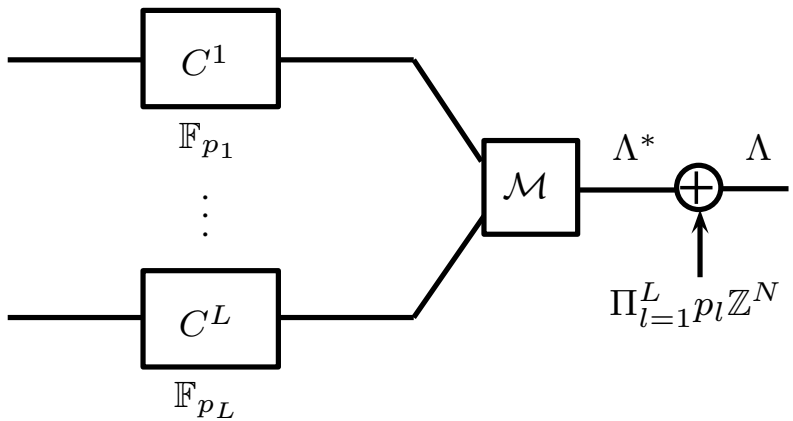
Product construction - L levels

1. Choose $(C^1, \ldots, C^L)$ independently (no nesting) where C^l is over $\mathbb{F}_{p_l}$

Construction π_A (previously called product construction)

Let $p_1, \ldots, p_L$ be distinct primes and $q = p_1\ p_2 \ldots p_L$.

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_L}$$



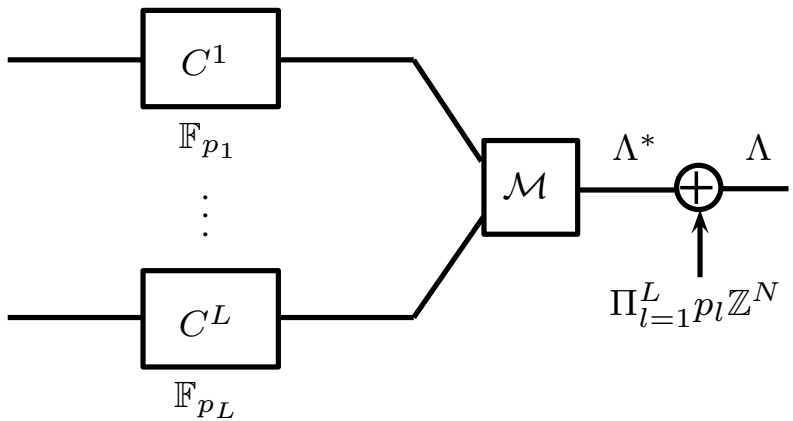
Product construction - L levels

1. Choose $(C^1, \ldots, C^L)$ independently (no nesting) where C^l is over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring isomorphism

Construction π_A (previously called product construction)

Let $p_1, \ldots, p_L$ be distinct primes and $q = p_1\ p_2 \ldots p_L$.

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_L}$$



Product construction - L levels

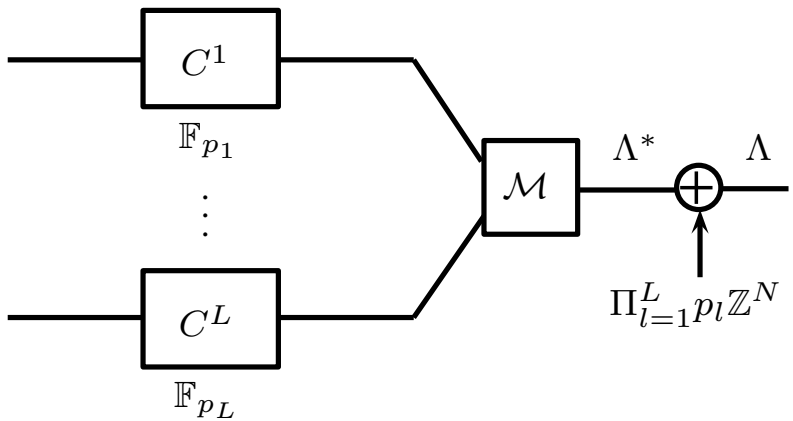
1. Choose $(C^1, \ldots, C^L)$ independently (no nesting) where C^l is over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring isomorphism
3. $\Lambda \triangleq \Lambda^* + q\mathbb{Z}^N$
4. $\boldsymbol{\lambda} \in \Lambda$ iff $\varphi(\boldsymbol{\lambda}) = (\mathbf{c}^1, \ldots, \mathbf{c}^L)$ where $\varphi \triangleq \mathcal{M}^{-1} \circ \bmod q\mathbb{Z}$

Works for other rings such as $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ (and $\mathfrak{O}_{\mathbb{K}}$ in general)

Construction π_A (previously called product construction)

Let $p_1, \ldots, p_L$ be distinct primes and $q = p_1\ p_2 \ldots p_L$.

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_L}$$



Product construction - L levels

1. Choose $(C^1, \ldots, C^L)$ independently (no nesting) where C^l is over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring isomorphism
3. $\Lambda \triangleq \Lambda^* + q\mathbb{Z}^N$
4. $\boldsymbol{\lambda} \in \Lambda$ iff $\varphi(\boldsymbol{\lambda}) = (\mathbf{c}^1, \ldots, \mathbf{c}^L)$ where $\varphi \triangleq \mathcal{M}^{-1} \circ \bmod q\mathbb{Z}$

Works for other rings such as $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ (and $\mathfrak{O}_{\mathbb{K}}$ in general)

Reduce to Construction A when $L = 1$

Connection to Construction A with Coding over Ring

Construction A with Coding over $\mathbb{Z}_q$

- C linear code over $\mathbb{Z}_q$ with a generator matrix $\mathbf{G}$
- $\tilde{\mathcal{M}} : \mathbb{Z}_q \to \mathbb{Z}$ natural mapping
- $\Lambda = \tilde{\mathcal{M}}(C) + q\mathbb{Z}^N = C + q\mathbb{Z}^N$

Construction π_A is in fact a special case of this construction:

- $q = p_1 \cdot p_2 \ldots \cdot p_L$
- For $z \in \mathbb{Z}_q$, $z = \mathcal{M}(z^1, \ldots, z^L)$ where $z^l \in \mathbb{F}_{p_l}$ if $z \mod p_l = z^l$
- $\mathbf{G} \mod p_l$ generates C^l for $l \in \{1, \ldots, L\}$

This is an interesting special case that has connection to multilevel coding/multistage decoding

Theorem 2

Exist Construction π_A lattices that are good for channel coding under multistage ML decoding

Proof.

- Follow the steps by Forney-Trott-Chung
- Modulo-$q\mathbb{Z}^N$ channel is symmetric (regular)
- Random multilevel linear codes achieve modulo-$q\mathbb{Z}^N$ channel capacity
- Let $q = p_1 p_2 \dots p_L$ tend to ∞

□

Theorem 3

Exist Construction π_A lattices that are good for MSE quantization

Proof.

- Follows the steps by Ordentlich-Erez
- Random multilevel linear codes induce uniform distribution over $\mathbb{R}^N$
- Let $q = p_1 p_2 \dots p_L$ tend to ∞

Power Constrained AWGN Channel: $\mathbf{y} = \mathbf{x} + \mathbf{z}$

Generalize Ordentlich-Erez's construction to multilevel lattices:

$$C_c^l = \{\mathbf{G}_c^l \odot \mathbf{w}^l | \mathbf{w}^l \in \mathbb{F}_{p_l}^{m_c^l}\}, \quad C_f^l = \{\mathbf{G}_f^l \odot \mathbf{w}^l | \mathbf{w}^l \in \mathbb{F}_{p_l}^{m_f^l}\},$$

$$\text{where} \quad \mathbf{G}_f^l = \begin{bmatrix} \mathbf{G}_c^l & \tilde{\mathbf{G}}^l \end{bmatrix},$$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^L) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^L) + \gamma \mathbb{Z}^N,$$

- Clearly, $C_c^l \subset C_f^l$; thus, $\Lambda_c \subset \Lambda_f$
- $C = \Lambda_f \cap \text{Vol}(\mathcal{V}_{\Lambda_c})$ with $R = \sum_{l=1}^{L} \frac{m_f^l - m_c^l}{N} \log(p_l)$
- Choose Λ_c good for MSE quantization and Λ_f good for coding
- Achieve AWGN capacity under multistage decoding

Low-complexity decoders

Serial modulo decoder (SMD):

- Stage 1: Form estimate of $\mathbf{c}^1$ from

$$\begin{aligned}\mathbf{y}^1 &= \mathbf{y} \mod p_1\mathbb{Z} \\ &= \left(\mathcal{M}(\mathbf{c}^1,\ldots,\mathbf{c}^L) + \Pi_{l=1}^{L} p_l\boldsymbol{\zeta} + \mathbf{z}\right) \mod p_1\mathbb{Z} \\ &= \left(\mathbf{c}^1 + \mathbf{z} \mod p_1\mathbb{Z}\right) \mod p_1\mathbb{Z} \text{ from CRT}\end{aligned}$$

- Stage s:
  - Subtract all the contribution from the previous decoded stages to get

$$\mathcal{M}(\mathbf{0},\ldots,\mathbf{0},\mathbf{c}^s,\ldots,\mathbf{c}^L) + \Pi_{l=1}^{L} p_l\boldsymbol{\zeta} + \mathbf{z}$$

  - Divide it by $\Pi_{l=1}^{s-1} p_l$ to get

$$\mathcal{M}(\mathbf{c}^s,\ldots,\mathbf{c}^L) + \Pi_{l=s}^{L} p_l\boldsymbol{\zeta} + \tilde{\mathbf{z}} \text{ Construction } \pi_A \text{ with } L-s+1 \text{ levels}$$

    where $\tilde{\mathbf{z}} \triangleq \mathbf{z}/\Pi_{l=1}^{s-1} p_l$
  - Form estimate of $\mathbf{c}^s$ from

$$\begin{aligned}\tilde{\mathbf{y}}^s &= \left(\mathcal{M}(\mathbf{c}^s,\ldots,\mathbf{c}^L) + \Pi_{l=s}^{L} p_l\boldsymbol{\zeta} + \tilde{\mathbf{z}}\right) \mod p_s\mathbb{Z} \\ &= \left(\mathbf{c}^s + \tilde{\mathbf{z}} \mod p_s\mathbb{Z}\right) \mod p_s\mathbb{Z} \text{ from CRT}\end{aligned}$$

Low-complexity decoders

Parallel modulo decoder (PMD):

- For $s \in \{1, \ldots, L\}$, simultaneously form

$$\begin{aligned}\mathbf{y}^s &= \mathbf{y} \mod p_s\mathbb{Z} \\ &= \left(\mathcal{M}(\mathbf{c}^1, \ldots, \mathbf{c}^L) + \Pi_{l=1}^{L} p_l \boldsymbol{\zeta} + \mathbf{z}\right) \mod p_s\mathbb{Z} \\ &= (\mathbf{c}_s + \mathbf{z} \mod p_s\mathbb{Z}) \mod p_s\mathbb{Z} \text{ from CRT}\end{aligned}$$

- Form estimate of $\mathbf{c}^s$ from $\mathbf{y}^s$
- More loss but substantially lower latency

Extensions

Construction π_D lattices:

- CRT only requires relatively prime rather than primes
- Allow all nature numbers: EX $12 = 4 \cdot 3$ hence $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_4 \times \mathbb{F}_3$
- Coding over rings for those levels which do not happen to be fields
- Construction D is a special case with only 1 level Feng-Silva-Kschischang
- Can only show goodness for channel coding so far

Multilevel lattices over algebraic integers:

- Every $\mathfrak{O}_{\mathbb{K}}$ forms a Dedekind domain
- Let $\mathfrak{I}$ be ideal s.t. $\mathfrak{I} = \Pi_{l=1}^{L} \mathfrak{p}_l$
- CRT: $\mathfrak{O}_{\mathbb{K}}/\mathfrak{I} \cong \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}_1 \times \ldots \times \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}_L \cong \mathbb{F}_{p_1^{f_1}} \times \ldots \times \mathbb{F}_{p_L^{f_L}}$

Outline

1 Construction A Lattices Review

2 Construction π_A Multilevel Lattices

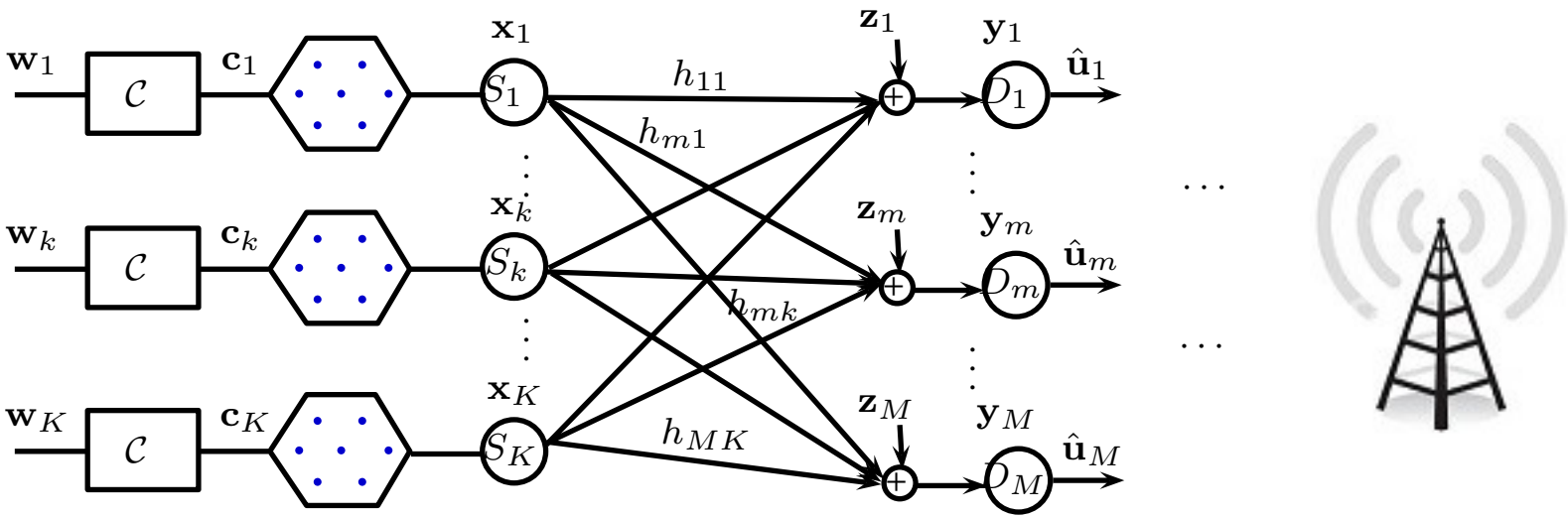
3 Application 1: Multistage Compute-and-Forward

4 Application 2: Lattice Index Coding

5 Future Directions

Lattice codes and a modern view of interference

Nazer-Gastpar, Compute-and-forward: Harnessing interference through structural codes, T-IT 11



- Source (S_k): Has message $\mathbf{w}_k$ over $\mathbb{F}_p$, where p is prime.
- Destination (D_m): $\mathbf{y}_m = \sum_{k=1}^{K} h_{mk}\mathbf{x}_k + \mathbf{z}_m$. No CSIT, only CSIR
- Recover $\mathbf{u}_m = \oplus_{k=1}^{K} b_{mk}\mathbf{w}_k$ where $b_{mk} \in \mathbb{F}_p$
- A building block of a large network

The Compute-and-Forward Paradigm

Theorem 4

Nazer-Gastpar For channel vector $\mathbf{h}_m \in \mathbb{R}^K$ and integer vector $\mathbf{a}_m \in \mathbb{Z}^K$, the following computation rate is achievable at D_m

$$R(\mathbf{h}_m, \mathbf{a}_m) = \frac{1}{2}\log^+\left(\frac{1+P\|\mathbf{h}_m\|^2}{\|\mathbf{a}_m\|^2 + P(\|\mathbf{h}_m\|^2\|\mathbf{a}_m\|^2 - (\mathbf{h}_m^T\mathbf{a}_m)^2)}\right)$$

How: To exploit the structural gains offered by the channel!

- Channel: $\mathbf{y}_m = \sum_{k=1}^K h_{mk}\mathbf{x}_k + \mathbf{z}_m$
- S_k: Use Construction A lattice code to match the channel structures to certain extent
- D_m: Directly decode to a linear integer combination of codewords
- e.g. $\sum_{k=1}^K a_{mk}\mathbf{x}_k$ where $a_{mk} \in \mathbb{Z}$
- Map this combination back to $\mathbf{u}_m = \oplus_{k=1}^K b_{mk} \odot \mathbf{w}_k$

Multistage Compute-and-Forward

Theorem 5

Same computation rate can be achieved with multistage decoding.

Proof.

- Split message into $\mathbf{w}_k^1 \times \ldots \times \mathbf{w}_k^L$ over $\mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_L}$
- Use the proposed multilevel lattices
- By CRT, uniquely represent $a_{mk} = \mathcal{M}(b_{mk}^1, \ldots, b_{mk}^L) + q\boldsymbol{\xi}$

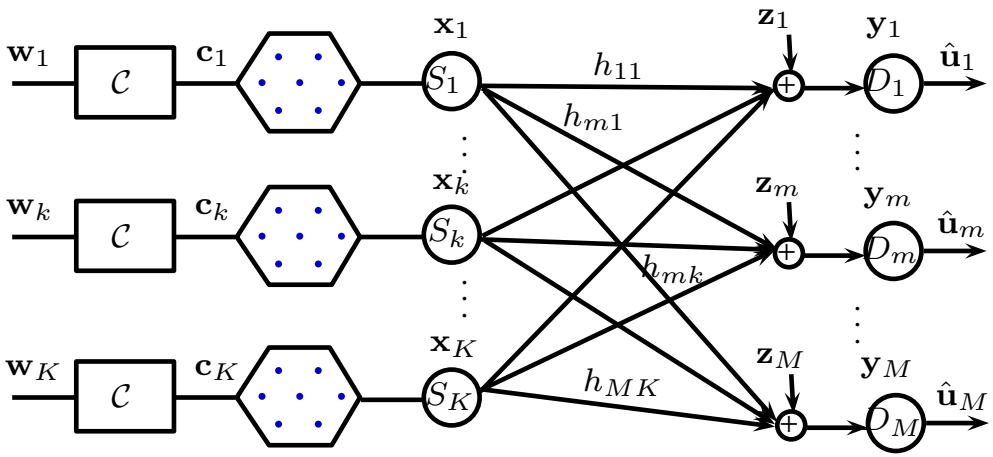
$$\begin{aligned}\sum_{k=1}^{K} a_{mk}\mathbf{x}_k &= \sum_{k=1}^{K} [\mathcal{M}(b_{mk}^1, \ldots, b_{mk}^L) + q\boldsymbol{\xi}] \cdot [\mathcal{M}(\mathbf{c}_k^1, \ldots, \mathbf{c}_k^L) + q\boldsymbol{\zeta}] \\ &= \mathcal{M}\left(\oplus_{k=1}^{K} b_{mk}^1 \odot \mathbf{c}_k^1, \ldots, \oplus_{k=1}^{K} b_{mk}^L \odot \mathbf{c}_k^L\right) + q\boldsymbol{\eta}\end{aligned}$$

- Decoding can be done level by level without losing optimality

□

Substantially reduce decoding complexity

Example of Multistage CF

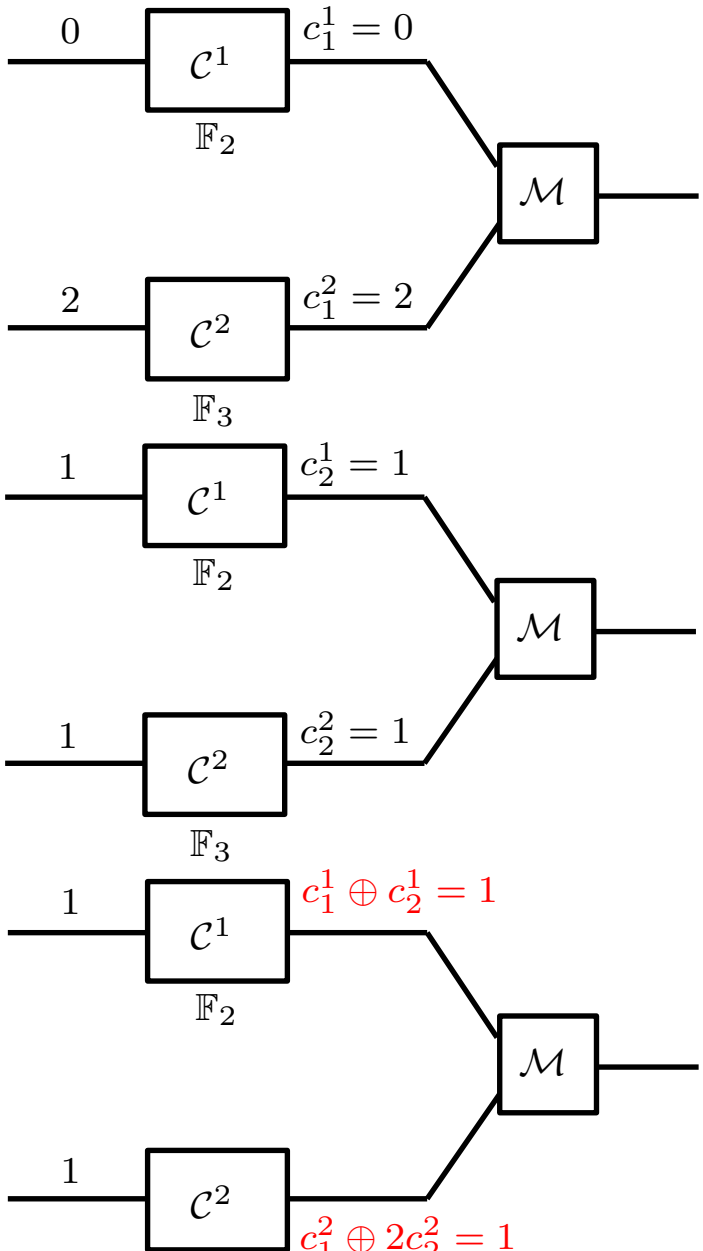


$$\mathbf{y} = \boxed{\mathbf{x}_1 + 5\mathbf{x}_2} + \mathbf{z}$$

- Consider $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$, same isomorphism

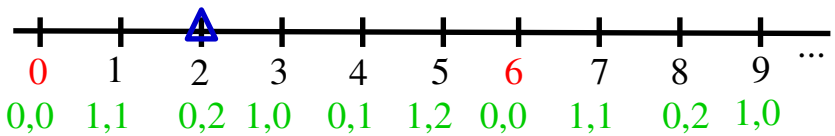
$$0 \leftrightarrow (0,0), \quad 1 \leftrightarrow (1,1), \quad 2 \leftrightarrow (0,2),$$
$$3 \leftrightarrow (1,0), \quad 4 \leftrightarrow (0,1), \quad 5 \leftrightarrow (1,2),$$

Example of Multistage CF



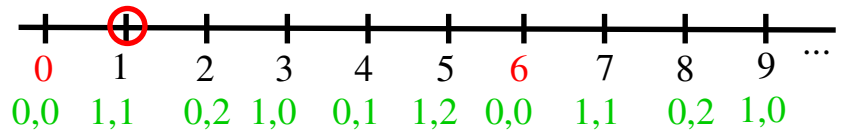
$h_1 = 1 = \mathcal{M}(1,1)$

$x_1 = \mathcal{M}(0,2) = 2$

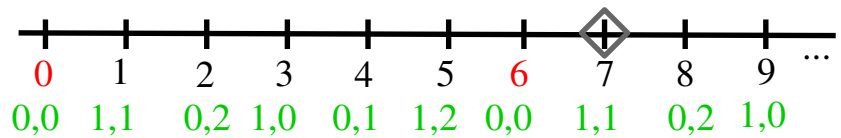


$h_2 = 5 = \mathcal{M}(1,2)$

$x_2 = \mathcal{M}(1,1) = 1$



$y = h_1 x_1 + h_2 x_2 = 7 = \mathcal{M}(1,1) + 6$



Outline

1 Construction A Lattices Review

2 Construction π_A Multilevel Lattices

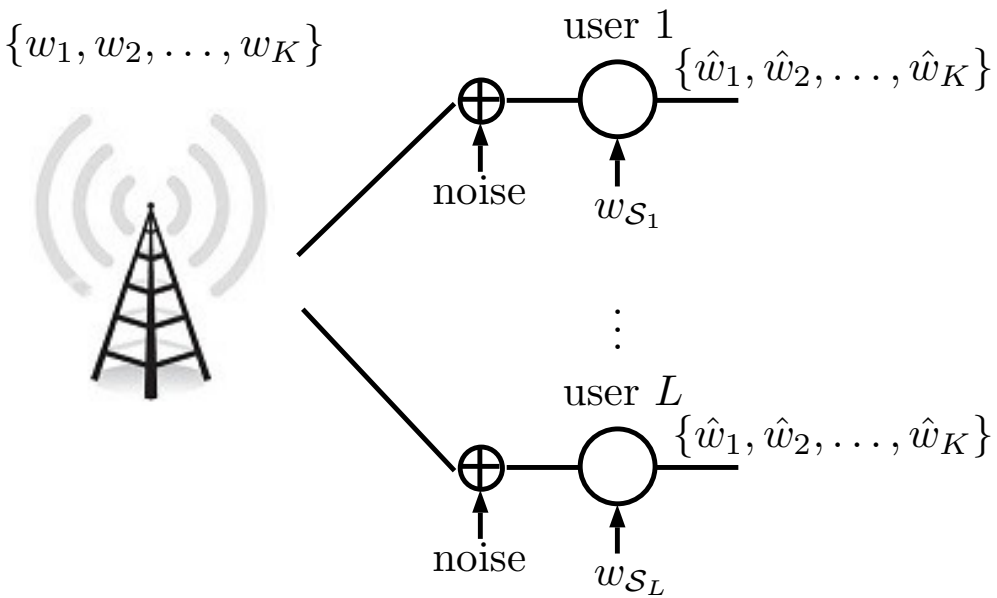
3 Application 1: Multistage Compute-and-Forward

4 Application 2: Lattice Index Coding

5 Future Directions

Broadcast channel with message side information

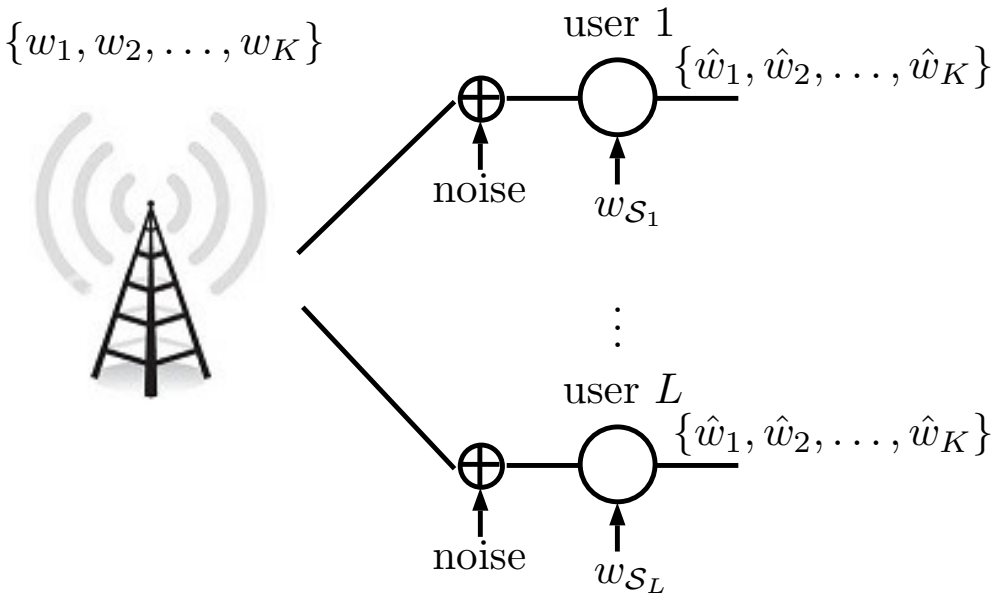
Natarajan-Hong-Viterbo T-IT 15



- Sender has independent messages $\{w_1, w_2, \ldots, w_K\}$.
- Each receiver requests all the messages
- Receiver l has $w_{\mathcal{S}_l}$ a set of side info described by index set $\mathcal{S}_l$
- For eg, $\mathcal{S}_1 = \{1, 2\}$, then $w_{\mathcal{S}_1} = \{w_1, w_2\}$
- Noisy network $\mathbf{y}_l = \mathbf{x} + \mathbf{z}_l$ where $\mathbb{E}[\mathbf{x}^2] \leq P$, and $\mathbf{z}_l \sim$ i.i.d. $\mathcal{N}(0, \rho_l^2)$

Broadcast channel with message side information

Natarajan-Hong-Viterbo T-IT 15



- Sender has independent messages $\{w_1, w_2, \ldots, w_K\}$.
- Each receiver requests all the messages
- Receiver l has $w_{\mathcal{S}_l}$ a set of side info described by index set $\mathcal{S}_l$
- For eg, $\mathcal{S}_1 = \{1, 2\}$, then $w_{\mathcal{S}_1} = \{w_1, w_2\}$
- Noisy network $\mathbf{y}_l = \mathbf{x} + \mathbf{z}_l$ where $\mathbb{E}[\mathbf{x}^2] \leq P$, and $\mathbf{z}_l \sim$ i.i.d. $\mathcal{N}(0, \rho_l^2)$

Noisy broadcasting problem with receiver side information

Capacity region and capacity-achieving codes

Capacity region (Tuncel T-IT 06): For every $l \in \{1, \ldots, L\}$,

$$\frac{1}{2}\log_2\left(1+\frac{P}{\rho_l^2}\right) > H(w_1, \ldots, w_K | w_{\mathcal{S}_l}) = \sum_{k=1}^{K} R_k - R_{\mathcal{S}_l}$$

- $R_{\mathcal{S}_l} = \sum_{k\in\mathcal{S}_l} R_k$
- Slepian-Wolf coding: Random codebooks + random binning + typicality

Capacity region and capacity-achieving codes

Capacity region (Tuncel T-IT 06): For every $l \in \{1, \ldots, L\}$,

$$\frac{1}{2}\log_2\left(1+\frac{P}{\rho_l^2}\right) > H(w_1, \ldots, w_K | w_{\mathcal{S}_l}) = \sum_{k=1}^{K} R_k - R_{\mathcal{S}_l}$$

- $R_{\mathcal{S}_l} = \sum_{k\in\mathcal{S}_l} R_k$
- Slepian-Wolf coding: Random codebooks + random binning + typicality

A good code should translate every bit of side info into 6 dB SNR reduction

Capacity region and capacity-achieving codes

Capacity region (Tuncel T-IT 06): For every $l \in \{1, \ldots, L\}$,

$$\frac{1}{2}\log_2\left(1+\frac{P}{\rho_l^2}\right) > H(w_1, \ldots, w_K | w_{\mathcal{S}_l}) = \sum_{k=1}^{K} R_k - R_{\mathcal{S}_l}$$

- $R_{\mathcal{S}_l} = \sum_{k\in\mathcal{S}_l} R_k$
- Slepian-Wolf coding: Random codebooks + random binning + typicality

A good code should translate every bit of side info into 6 dB SNR reduction

Lattice index codes by Natarajan-Hong-Viterbo T-IT 15

- Uniform side info gain of 6 dB by exploiting algebraic structure of CRT
- Extension to general ring of algebraic integers, Huang T-IT submitted 15
- Obtain diversity gains on top of side information gains

CRT seems to provide a right structure for this problem

Capacity-achieving lattice index codes

- Let $w_k \in \mathbb{F}_{p_k}$, $k \in \{1, \ldots, K\}$
- Encode the messages by $C = \Lambda_f \cap \mathsf{Vol}(\mathcal{V}_{\Lambda_c})$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^k, \ldots, C_f^K) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^k, \ldots, C_c^K) + \gamma \mathbb{Z}^N,$$

- Here, $\mathcal{M}(v^1, \ldots, v^L) \triangleq q_1 v^1 + \ldots + q_L v^L \mod q\mathbb{Z}$
- Receiver l sees a codebook with messages in $\mathcal{S}_l$ fixed

Example 6 (3-User Case. $\mathcal{S}_1 = \{1\}$, $\mathcal{S}_2 = \{2, 3\}$, $\mathcal{S}_3 = \{1, 3\}$)

$$\Lambda_f = \gamma q^{-1} \mathcal{M}(C_f^1, C_f^2, C_f^3) + \gamma \mathbb{Z}^N$$
$$\Lambda_c = \gamma q^{-1} \mathcal{M}(C_c^1, C_c^2, C_c^3) + \gamma \mathbb{Z}^N$$

Capacity-achieving lattice index codes

- Let $w_k \in \mathbb{F}_{p_k}$, $k \in \{1, \ldots, K\}$
- Encode the messages by $C = \Lambda_f \cap \mathsf{Vol}(\mathcal{V}_{\Lambda_c})$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^k, \ldots, C_f^K) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^k, \ldots, C_c^K) + \gamma \mathbb{Z}^N,$$

- Here, $\mathcal{M}(v^1, \ldots, v^L) \triangleq q_1 v^1 + \ldots + q_L v^L \mod q\mathbb{Z}$
- Receiver l sees a codebook with messages in $\mathcal{S}_l$ fixed

Example 6 (3-User Case. $\mathcal{S}_1 = \{1\}$, $\mathcal{S}_2 = \{2, 3\}$, $\mathcal{S}_3 = \{1, 3\}$)

$$\Lambda_f = \gamma q^{-1} \mathcal{M}(C_f^1, C_f^2, C_f^3) + \gamma \mathbb{Z}^N$$
$$\Lambda_c = \gamma q^{-1} \mathcal{M}(C_c^1, C_c^2, C_c^3) + \gamma \mathbb{Z}^N$$

$R_2 + R_3 \leq \frac{1}{2} \log(1 + P/\rho_1^2)$ if Λ_f with C_f^1 fixed is good for coding

Capacity-achieving lattice index codes

- Let $w_k \in \mathbb{F}_{p_k}$, $k \in \{1, \ldots, K\}$
- Encode the messages by $C = \Lambda_f \cap \mathsf{Vol}(\mathcal{V}_{\Lambda_c})$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^k, \ldots, C_f^K) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^k, \ldots, C_c^K) + \gamma \mathbb{Z}^N,$$

- Here, $\mathcal{M}(v^1, \ldots, v^L) \triangleq q_1 v^1 + \ldots + q_L v^L \mod q\mathbb{Z}$
- Receiver l sees a codebook with messages in $\mathcal{S}_l$ fixed

Example 6 (3-User Case. $\mathcal{S}_1 = \{1\}$, $\mathcal{S}_2 = \{2, 3\}$, $\mathcal{S}_3 = \{1, 3\}$)

$$\Lambda_f = \gamma q^{-1} \mathcal{M}(C_f^1, C_f^2, C_f^3) + \gamma \mathbb{Z}^N$$
$$\Lambda_c = \gamma q^{-1} \mathcal{M}(C_c^1, C_c^2, C_c^3) + \gamma \mathbb{Z}^N$$

$R_1 \leq \frac{1}{2} \log(1 + P/\rho_2^2)$ if Λ_f with C_f^2 and C_f^3 fixed is good for coding

Capacity-achieving lattice index codes

- Let $w_k \in \mathbb{F}_{p_k}$, $k \in \{1, \ldots, K\}$
- Encode the messages by $C = \Lambda_f \cap \mathsf{Vol}(\mathcal{V}_{\Lambda_c})$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^k, \ldots, C_f^K) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^k, \ldots, C_c^K) + \gamma \mathbb{Z}^N,$$

- Here, $\mathcal{M}(v^1, \ldots, v^L) \triangleq q_1 v^1 + \ldots + q_L v^L \mod q\mathbb{Z}$
- Receiver l sees a codebook with messages in $\mathcal{S}_l$ fixed

Example 6 (3-User Case. $\mathcal{S}_1 = \{1\}$, $\mathcal{S}_2 = \{2, 3\}$, $\mathcal{S}_3 = \{1, 3\}$)

$$\Lambda_f = \gamma q^{-1} \mathcal{M}(C_f^1, C_f^2, C_f^3) + \gamma \mathbb{Z}^N$$
$$\Lambda_c = \gamma q^{-1} \mathcal{M}(C_c^1, C_c^2, C_c^3) + \gamma \mathbb{Z}^N$$

$R_2 \leq \frac{1}{2} \log(1 + P/\rho_3^2)$ if Λ_f with C_f^1 and C_f^3 fixed is good for coding

Capacity-achieving lattice index codes

- Let $w_k \in \mathbb{F}_{p_k}$, $k \in \{1, \ldots, K\}$
- Encode the messages by $C = \Lambda_f \cap \mathsf{Vol}(\mathcal{V}_{\Lambda_c})$

$$\Lambda_f \triangleq \gamma q^{-1} \mathcal{M}(C_f^1, \ldots, C_f^k, \ldots, C_f^K) + \gamma \mathbb{Z}^N,$$
$$\Lambda_c \triangleq \gamma q^{-1} \mathcal{M}(C_c^1, \ldots, C_c^k, \ldots, C_c^K) + \gamma \mathbb{Z}^N,$$

- Here, $\mathcal{M}(v^1, \ldots, v^L) \triangleq q_1 v^1 + \ldots + q_L v^L \mod q\mathbb{Z}$
- Receiver l sees a codebook with messages in $\mathcal{S}_l$ fixed

Example 6 (3-User Case. $\mathcal{S}_1 = \{1\}$, $\mathcal{S}_2 = \{2, 3\}$, $\mathcal{S}_3 = \{1, 3\}$)

$$\Lambda_f = \gamma q^{-1} \mathcal{M}(C_f^1, C_f^2, C_f^3) + \gamma \mathbb{Z}^N$$
$$\Lambda_c = \gamma q^{-1} \mathcal{M}(C_c^1, C_c^2, C_c^3) + \gamma \mathbb{Z}^N$$

In general, need good Construction π_A lattices with arbitrary levels fixed

Sketch of the proof

Consider 2 levels: $\Lambda = p_2 C^1 + p_1 C^2 + p_1 p_2 \mathbb{Z}^N$. Note that

$$\begin{aligned}\Lambda &= p_1 C^2 + p_2 \left(C^1 + p_1 \mathbb{Z}^N\right) = p_1 C^2 + p_2 \Lambda_1 \\ &= p_2 C^1 + p_1 \left(C^2 + p_2 \mathbb{Z}^N\right) = p_2 C^1 + p_1 \Lambda_2\end{aligned}$$

- Randomly picking C^1 results in good Λ_1 w.h.p.
- Randomly picking C^2 results in good Λ_2 w.h.p.

Sketch of the proof

Consider 2 levels: $\Lambda = p_2 C^1 + p_1 C^2 + p_1 p_2 \mathbb{Z}^N$. Note that

$$\begin{aligned}\Lambda &= p_1 C^2 + p_2 \left(C^1 + p_1 \mathbb{Z}^N\right) = p_1 C^2 + p_2 \Lambda_1 \\ &= p_2 C^1 + p_1 \left(C^2 + p_2 \mathbb{Z}^N\right) = p_2 C^1 + p_1 \Lambda_2\end{aligned}$$

- Randomly picking C^1 results in good Λ_1 w.h.p.
- Randomly picking C^2 results in good Λ_2 w.h.p.

- Note that $p_2 \Lambda_1 \subset \Lambda \subset \Lambda_1$
- Λ can be viewed as a Construction A lattice over base lattice Λ_1
- Tailor (Loeliger's version) Minkowski-Hlawka theorem specifically for this construction
  - So picking C^2 randomly results in good Λ w.h.p.

Outline

1 Construction A Lattices Review

2 Construction π_A Multilevel Lattices

3 Application 1: Multistage Compute-and-Forward

4 Application 2: Lattice Index Coding

5 Future Directions

Future Directions

Construction π_A lattices:

Seeking for interesting problems where Construction π_A can be useful

Future Directions

Construction π_A lattices:

Seeking for interesting problems where Construction π_A can be useful

Number field lattices:

Construction A lattice codes over a general $\mathfrak{O}_{\mathbb{K}}$

- Kositwattanarerk-Ong-Oggier: Block fading wiretap channel
- Campello-Ling-Belfiore: Compound block fading channel
- Huang-Narayanan-Wang: Adaptive compute-and-forward

CF over block fading channel

RX: $[\mathbf{y}_m^{(1)}, \ldots, \mathbf{y}_m^{(B)}]$ where $\mathbf{y}_m^{(b)} = \sum_{k=1}^{K} h_{mk}^{(b)} \mathbf{x}_k^{(b)} + \mathbf{z}_m^{(b)}$

- Construct lattice code from $\mathfrak{O}_{\mathbb{K}}$ where $\mathbb{K}$ has degree B
- $\mathcal{M} : \mathbb{F}_{p^f} \to \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}$ ring isomorphism
- $\tilde{\Lambda} = \mathcal{M}(C) + \mathfrak{p}^n$ and $\Lambda = \Psi(\tilde{\Lambda})$ where Ψ is canonical embedding
- $\boldsymbol{\lambda} = \Psi(\tilde{\boldsymbol{\lambda}}) = [\sigma_1(\tilde{\boldsymbol{\lambda}}), \ldots, \sigma_B(\tilde{\boldsymbol{\lambda}})]$
- Enable computing

$$\left[\sum_{k=1}^{K} a_{mk}^{(1)} \mathbf{x}_k^{(1)}, \ldots, \sum_{k=1}^{K} a_{mk}^{(B)} \mathbf{x}_k^{(B)}\right] \quad \text{where} \quad \Psi^{-1}([a_{mk}^{(1)}, \ldots, a_{mk}^{(B)}]) \in \mathfrak{O}_{\mathbb{K}}$$

- Seem to better match channel's structure than $\mathbb{Z}$-lattices

CF over block fading channel

RX: $[\mathbf{y}_m^{(1)}, \ldots, \mathbf{y}_m^{(B)}]$ where $\mathbf{y}_m^{(b)} = \sum_{k=1}^{K} h_{mk}^{(b)} \mathbf{x}_k^{(b)} + \mathbf{z}_m^{(b)}$

- Construct lattice code from $\mathfrak{O}_{\mathbb{K}}$ where $\mathbb{K}$ has degree B
- $\mathcal{M} : \mathbb{F}_{p^f} \to \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}$ ring isomorphism
- $\tilde{\Lambda} = \mathcal{M}(C) + \mathfrak{p}^n$ and $\Lambda = \Psi(\tilde{\Lambda})$ where Ψ is canonical embedding
- $\boldsymbol{\lambda} = \Psi(\tilde{\boldsymbol{\lambda}}) = [\sigma_1(\tilde{\boldsymbol{\lambda}}), \ldots, \sigma_B(\tilde{\boldsymbol{\lambda}})]$
- Enable computing

$$\left[\sum_{k=1}^{K} a_{mk}^{(1)} \mathbf{x}_k^{(1)}, \ldots, \sum_{k=1}^{K} a_{mk}^{(B)} \mathbf{x}_k^{(B)}\right] \quad \text{where} \quad \Psi^{-1}([a_{mk}^{(1)}, \ldots, a_{mk}^{(B)}]) \in \mathfrak{O}_{\mathbb{K}}$$

- Seem to better match channel's structure than $\mathbb{Z}$-lattices

Good for coding has been proved by Campello-Ling-Belfiore. Need to show good for MSE quantization

CF over block fading channel

RX: $[\mathbf{y}_m^{(1)}, \ldots, \mathbf{y}_m^{(B)}]$ where $\mathbf{y}_m^{(b)} = \sum_{k=1}^{K} h_{mk}^{(b)} \mathbf{x}_k^{(b)} + \mathbf{z}_m^{(b)}$

- Construct lattice code from $\mathfrak{O}_{\mathbb{K}}$ where $\mathbb{K}$ has degree B
- $\mathcal{M} : \mathbb{F}_{p^f} \to \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}$ ring isomorphism
- $\tilde{\Lambda} = \mathcal{M}(C) + \mathfrak{p}^n$ and $\Lambda = \Psi(\tilde{\Lambda})$ where Ψ is canonical embedding
- $\boldsymbol{\lambda} = \Psi(\tilde{\boldsymbol{\lambda}}) = [\sigma_1(\tilde{\boldsymbol{\lambda}}), \ldots, \sigma_B(\tilde{\boldsymbol{\lambda}})]$
- Enable computing

$$\left[\sum_{k=1}^{K} a_{mk}^{(1)} \mathbf{x}_k^{(1)}, \ldots, \sum_{k=1}^{K} a_{mk}^{(B)} \mathbf{x}_k^{(B)}\right] \quad \text{where} \quad \Psi^{-1}([a_{mk}^{(1)}, \ldots, a_{mk}^{(B)}]) \in \mathfrak{O}_{\mathbb{K}}$$

- Seem to better match channel's structure than $\mathbb{Z}$-lattices

Good for coding has been proved by Campello-Ling-Belfiore. Need to show good for MSE quantization

Chinese Remainder Theorem

Let $p_1, p_2, \ldots, p_L$ be L distinct co-prime integers and $q = p_1.p_2.\ldots.p_L$. Then, given

$$\begin{aligned} x &\equiv a_1 (\text{mod} p_1) \\ x &\equiv a_2 (\text{mod} p_2) \\ &\vdots \\ x &\equiv a_L (\text{mod} p_L) \end{aligned}$$

there exists exactly one $x \in \mathbb{Z}_q$ satisfying this system.

Chinese Remainder Theorem

Let $p_1, p_2, \ldots, p_L$ be L distinct co-prime integers and $q = p_1.p_2.\ldots.p_L$. Then, given

$$\begin{aligned} x &\equiv a_1 (\text{mod} p_1) \\ x &\equiv a_2 (\text{mod} p_2) \\ &\vdots \\ x &\equiv a_L (\text{mod} p_L) \end{aligned}$$

there exists exactly one $x \in \mathbb{Z}_q$ satisfying this system.

EX: $q = 6$, $p_1 = 2$, $p_2 = 3$

$$\begin{aligned} x &\equiv 0 (\text{mod} 2) \\ x &\equiv 1 (\text{mod} 3) \end{aligned}$$

$$\boxed{x = 4}$$

Modified M.-H. Theorem

Consider $\Lambda = p_2 C^1 + p_1 C^2 + p_1 p_2 \mathbb{Z}^n = p_1 C^2 + p_2 \Lambda_1$

- Let $\mathcal{M}_2(v^2) \triangleq p_1 v^2 \mod p_2 \Lambda_1$ where $v^2 \in \mathbb{F}_{p_2}$
- Let $\sigma \triangleq \mathcal{M}^{-1} \circ \mod p_2 \Lambda_1$
- Let $\mathcal{C}^2$ be the ensemble of (N, k_2) linear codes over $\mathbb{F}_{p_2}$

$$\frac{1}{|\mathcal{C}^2|} \sum_{C^2 \in \mathcal{C}^2} \sum_{\mathbf{v} \in \gamma\Lambda \setminus \mathbf{0}} f(\mathbf{v})$$

$$= \frac{1}{|\mathcal{C}^2|} \sum_{C^2 \in \mathcal{C}^2} \left[\sum_{\mathbf{v} \in \Lambda_1 \setminus \mathbf{0} : \sigma(\mathbf{v}) = \mathbf{0}} f(\gamma \mathbf{v}) + \sum_{\mathbf{v} \in \Lambda_1 \setminus \mathbf{0} : \sigma(\mathbf{v}) \in C^2 \setminus \mathbf{0}} f(\gamma \mathbf{v}) \right]$$

$$= \sum_{\mathbf{v} \in \Lambda_1 \setminus \mathbf{0} : \sigma(\mathbf{v}) = \mathbf{0}} f(\gamma \mathbf{v}) + \frac{1}{|\mathcal{C}^2|} \sum_{C^2 \in \mathcal{C}^2} \sum_{\mathbf{c} \in C^2 \setminus \mathbf{0}} \left[\sum_{\mathbf{v} \in \Lambda_1 : \sigma(\mathbf{v}) = \mathbf{c}} f(\gamma \mathbf{v}) \right]$$

$$= \sum_{\mathbf{v}\in\Lambda_1\setminus\mathbf{0}:\sigma(\mathbf{v})=\mathbf{0}} f(\gamma\mathbf{v}) + \frac{p_2^{k_2}-1}{p_2^N-1} \sum_{\mathbf{c}\in\mathbb{F}_{p_2}^N} \left[\sum_{\mathbf{v}\in\Lambda_1:\sigma(\mathbf{v})=\mathbf{c}} f(\gamma\mathbf{v}) \right]$$

$$= \sum_{\mathbf{v}\in\Lambda_1\setminus\mathbf{0}:\sigma(\mathbf{v})=\mathbf{0}} f(\gamma\mathbf{v}) + \frac{p_2^{k_2}-1}{p_2^N-1} \sum_{\mathbf{v}\in\Lambda_1:\sigma(\mathbf{v})\neq\mathbf{0}} f(\gamma\mathbf{v})$$

$$\overset{(a)}{\approx} p_2^{k_2-N}\gamma^{-N}\mathsf{Vol}(\mathcal{V}_{\Lambda_1})^{-1} \sum_{\mathbf{v}\in\gamma\Lambda_1:\sigma(\mathbf{v})\neq\mathbf{0}} f(\mathbf{v})\gamma^N\mathsf{Vol}(\mathcal{V}_{\Lambda_1})$$

$$\overset{(b)}{\approx} \mathsf{Vol}(\mathcal{V}_{\gamma\Lambda})^{-1} \int_{\mathbb{R}^N} f(\mathbf{v})d\mathbf{v},$$

- (a) requires p_2 large and $f(.)$ bounded
- (b) requires $\gamma^N\mathsf{Vol}(\mathcal{V}_{\Lambda_1})$ small s.t. Riemann sum $\rightarrow$ Riemann integration
- $\mathsf{Vol}(\mathcal{V}_{\gamma\Lambda}) = \gamma^N p_2^{k_2-N}\mathsf{Vol}(\mathcal{V}_{\Lambda_1})^{-1} = p_2^{k_2-N}p_1^{k_1-N}$