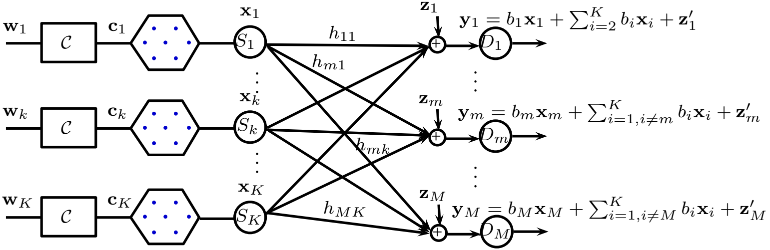
Multilevel Coding and Modulation for Interference Channels, Integer-Forcing, Compute-and-Forward, Physical Layer Network Coding

Yu-Chih Huang, Avinash Vem & Krishna R. Narayanan
Texas A&M University

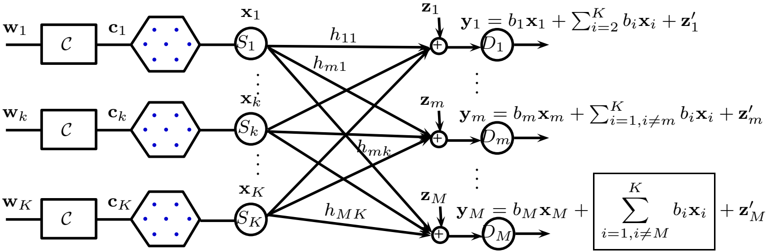
Lattice codes and a modern view of interference

- A new perspective for dealing with interference is emerging
- Integer combinations of interfering codewords are directly decoded
- Lattice codes are at the heart of these coding schemes

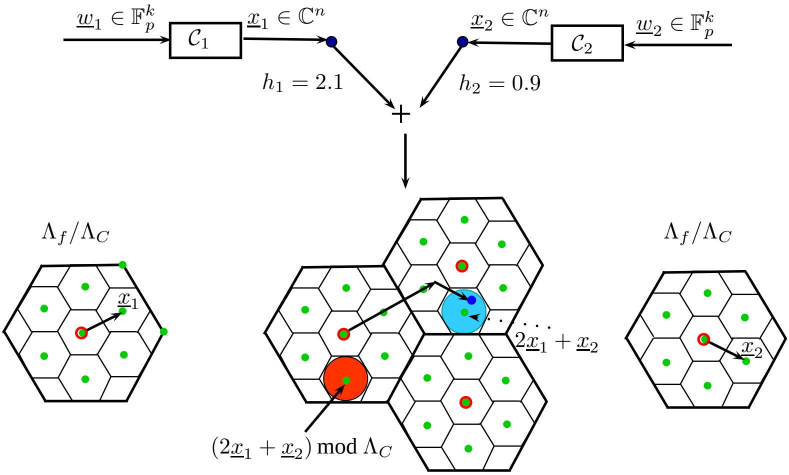


Lattice codes and a modern view of interference

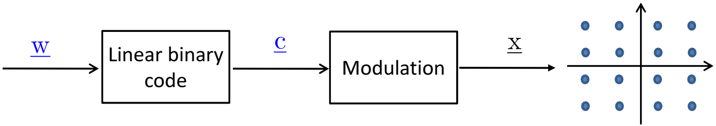
- A new perspective for dealing with interference is emerging
- Integer combinations of interfering codewords are directly decoded
- Lattice codes are at the heart of these coding schemes



Lattices, Lattice Codes and Integer Combinations

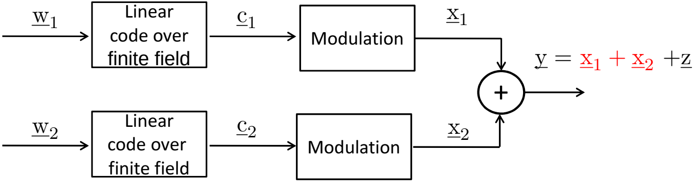


Coding and Modulation for Single User Channels

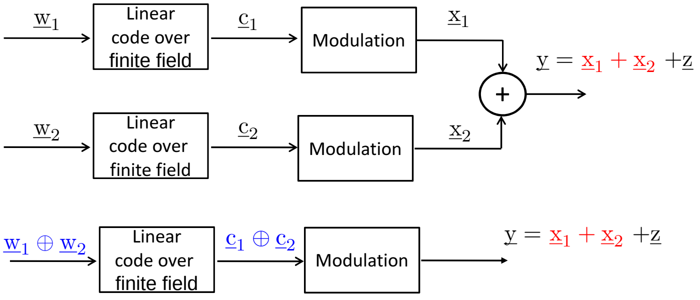


- We mostly understand how to design codes - Turbo, LDPC etc
- Codes are designed over the finite field - e.g. binary codes
- We also understand the interface between coding and modulation
- Bit interleaved coded modulation, multilevel coded modulation etc

Coding and Modulation for Decoding Linear Combinations

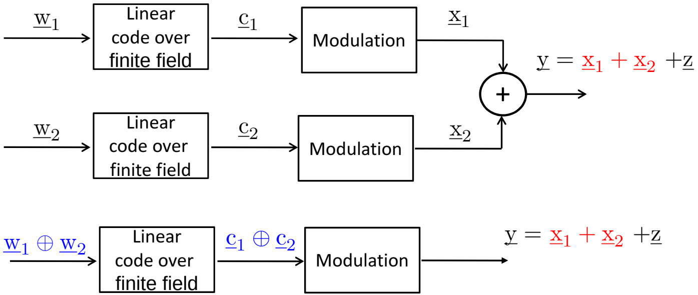


Coding and Modulation for Decoding Linear Combinations



- When is it efficient to decode $\underline{c}_1 \oplus \underline{c}_2$ from $\underline{y}$?
- When are linear comb. over the finite field related to those over real field?

Coding and Modulation for Decoding Linear Combinations



- When is it efficient to decode $\underline{c}_1 \oplus \underline{c}_2$ from $\underline{y}$?
- When are linear comb. over the finite field related to those over real field?
- Binary codes + QAM does not work

Algebra - Rings

$\{\mathcal{R}, \oplus, \odot\}$ is a commutative ring

- $\mathcal{R}$ is closed under $\oplus$, has an identity and has an inverse
- $\mathcal{R}$ is closed under $\odot$, may not have identity and inverse

Examples

- Ring of integers - $\mathbb{Z}$ - set of integers with ordinary $+, \times$
- Ring of integers mod p - $\mathbb{Z}_p \triangleq \{0, 1, 2, \ldots, p-1\}$, $+$ mod p, $\times$ mod p

Algebra - Rings

$\{\mathcal{R}, \oplus, \odot\}$ is a commutative ring

- $\mathcal{R}$ is closed under $\oplus$, has an identity and has an inverse
- $\mathcal{R}$ is closed under $\odot$, may not have identity and inverse

Examples

- Ring of integers - $\mathbb{Z}$ - set of integers with ordinary $+, \times$
- Ring of integers mod p - $\mathbb{Z}_p \triangleq \{0, 1, 2, \ldots, p-1\}$, $+$ mod p, $\times$ mod p
- $\mathbb{Z}_6 \triangleq \{0, 1, 2, 3, 4, 5\}$, $+$ mod 6, $\times$ mod 6
  - 2 does not have an inverse

Algebra - Fields

$\{\mathbb{F}, \oplus, \odot\}$ is a field

- $\mathbb{F}$ is closed under $\oplus$, has an identity 0, and an inverse
- $\mathbb{F} - \{0\}$ is closed under $\odot$, has an identity and an inverse

EX: $\mathbb{Z}_p \triangleq \{0, 1, \ldots, p-1\}$, $+$ mod p, $\times$ mod p is a field if p is prime

- $\mathbb{Z}_p \cong \mathbb{F}_p$ if p is prime
- $\mathbb{Z}_p$ is only a ring otherwise

Algebra - Fields

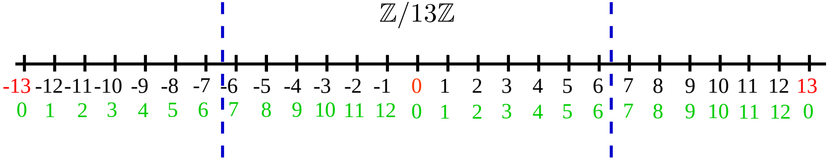
$\{\mathbb{F}, \oplus, \odot\}$ is a field

- $\mathbb{F}$ is closed under $\oplus$, has an identity 0, and an inverse
- $\mathbb{F} - \{0\}$ is closed under $\odot$, has an identity and an inverse

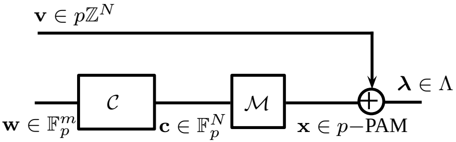
EX: $\mathbb{Z}_p \triangleq \{0, 1, \ldots, p-1\}$, $+$ mod p, $\times$ mod p is a field if p is prime

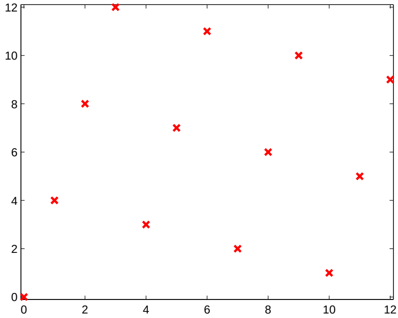
- $\mathbb{Z}_p \cong \mathbb{F}_p$ if p is prime
- $\mathbb{Z}_p$ is only a ring otherwise

13-PAM $+$ mod 13 is equivalent to decoding over $\mathbb{F}_{13}$



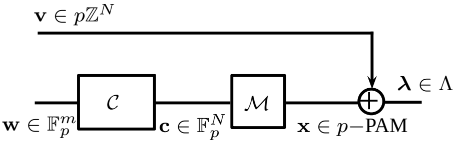
N-Dimensional Lattice Using Construction A



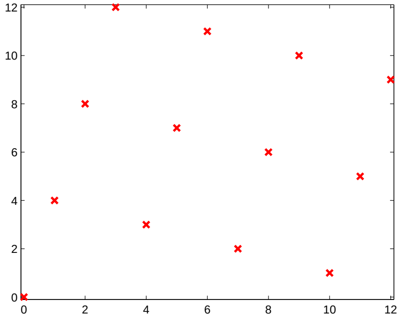


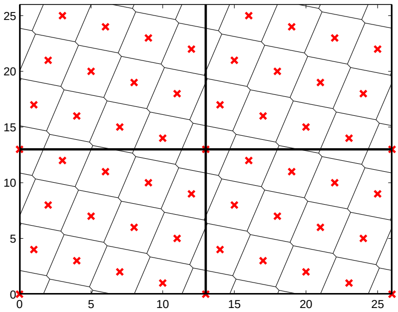
- C linear code over $\mathbb{F}_p$ (e.g., 13)
- Ex: $n = 2, m = 1$, code $\mathbf{G} = [1\ 4]$
- $\mathcal{M} : \mathbb{F}_p \to \mathbb{Z}$ trivial mapping
- $\lambda \in \Lambda$ iff $\lambda \bmod p\mathbb{Z} \in C$
- $\lambda = \mathcal{M}(\underline{c}) + p\underline{k}$ - integer vector k

N-Dimensional Lattice Using Construction A



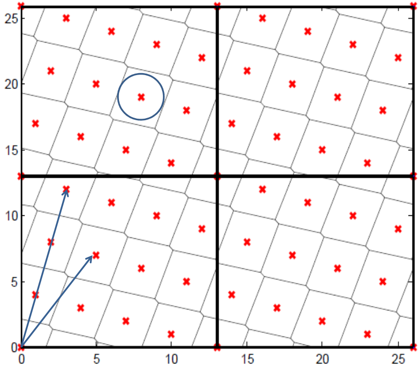
- C linear code over $\mathbb{F}_p$ (e.g., 13)
- Ex: $n = 2, m = 1$, code $\mathbf{G} = [1\ 4]$
- $\mathcal{M} : \mathbb{F}_p \to \mathbb{Z}$ trivial mapping
- $\lambda \in \Lambda$ iff $\lambda \bmod p\mathbb{Z} \in C$
- $\lambda = \mathcal{M}(\underline{c}) + p\underline{k}$ - integer vector k





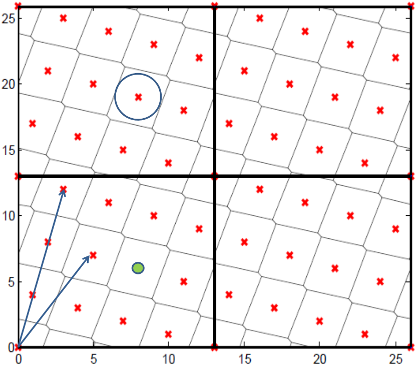
What makes this a Lattice?

- $\underline{x}_1 = \mathcal{M}(\underline{c}_1) + \underline{k}_1 p, k_1 \in \mathbb{Z}^n$
- $\underline{x}_2 = \mathcal{M}(\underline{c}_2) + \underline{k}_2 p, k_2 \in \mathbb{Z}^n$
- $\boxed{\underline{x}_1 + \underline{x}_2 = \mathcal{M}(\underline{c}_1 \oplus \underline{c}_2) + \underline{k}_3 p}$
- $\boxed{(\underline{x}_1 + \underline{x}_2) \text{ mod } p = \mathcal{M}(c_1 \oplus c_2)}$



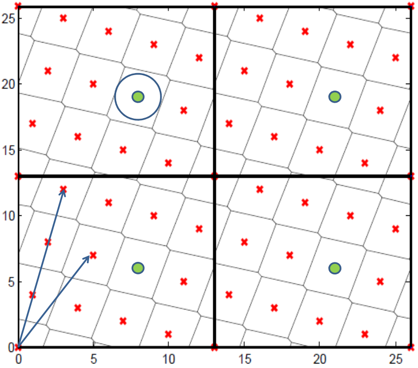
What makes this a Lattice?

- $\underline{x}_1 = \mathcal{M}(\underline{c}_1) + \underline{k}_1 p, k_1 \in \mathbb{Z}^n$
- $\underline{x}_2 = \mathcal{M}(\underline{c}_2) + \underline{k}_2 p, k_2 \in \mathbb{Z}^n$
- $\boxed{\underline{x}_1 + \underline{x}_2 = \mathcal{M}(\underline{c}_1 \oplus \underline{c}_2) + \underline{k}_3 p}$
- $\boxed{(\underline{x}_1 + \underline{x}_2) \bmod p = \mathcal{M}(c_1 \oplus c_2)}$

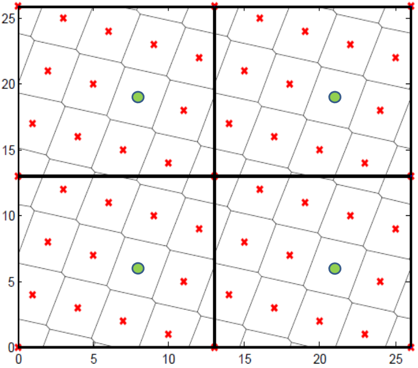


What makes this a Lattice?

- $\underline{x}_1 = \mathcal{M}(\underline{c}_1) + \underline{k}_1 p, k_1 \in \mathbb{Z}^n$
- $\underline{x}_2 = \mathcal{M}(\underline{c}_2) + \underline{k}_2 p, k_2 \in \mathbb{Z}^n$
- $\boxed{\underline{x}_1 + \underline{x}_2 = \mathcal{M}(\underline{c}_1 \oplus \underline{c}_2) + \underline{k}_3 p}$
- $\boxed{(\underline{x}_1 + \underline{x}_2) \text{ mod } p = \mathcal{M}(c_1 \oplus c_2)}$

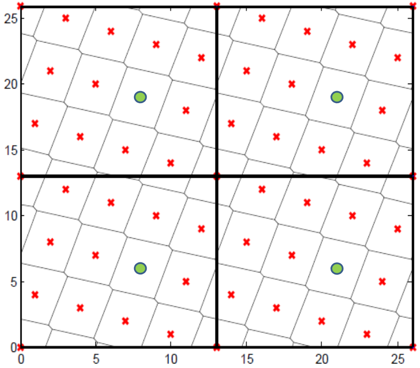


Problem with Construction A



- p has to be large to have a good lattice, Loeliger, Erez et al
- Complexity depends on decoding the linear code over $\mathbb{F}_p$, e.g. $p \log p$
- For e.g., simulation results by di Pietro, Boutros, Zemor, Brunel with $\mathbb{F}_{41}$

Problem with Construction A



- p has to be large to have a good lattice, Loeliger, Erez et al
- Complexity depends on decoding the linear code over $\mathbb{F}_p$, e.g. $p \log p$
- For e.g., simulation results by di Pietro, Boutros, Zemor, Brunel with $\mathbb{F}_{41}$
- Optimal lattices under ML decoding - no proof yet under iterative decoding

Main Result in This Talk

Interesting extensions to 2-D constellations

Main Result in This Talk

Interesting extensions to 2-D constellations

Complexity can be substantially decreased

- Inspired by Feng, Silva and Kschischang'10
- p does not have to be prime - can be replaced by $p_1 p_2 \ldots p_L$
- Instead of working over $\mathbb{F}_p$, we can work over $\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \ldots \times \mathbb{F}_{p_l}$
- Complexity decreases from $p_1 p_2 \ldots p_L \log(p_1 p_2 \ldots p_L)$ to $\sum_i p_i \log p_i$
- Ex: $p = 210$ 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

Main Result in This Talk

Interesting extensions to 2-D constellations

Complexity can be substantially decreased

- Inspired by Feng, Silva and Kschischang'10
- p does not have to be prime - can be replaced by $p_1 p_2 \ldots p_L$
- Instead of working over $\mathbb{F}_p$, we can work over $\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \ldots \times \mathbb{F}_{p_l}$
- Complexity decreases from $p_1 p_2 \ldots p_L \log(p_1 p_2 \ldots p_L)$ to $\sum_i p_i \log p_i$
- Ex: $p = 210$ 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

Nested binary codes suffice

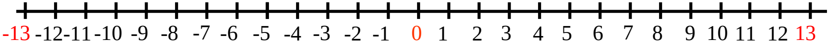
- Construction-D lattices are optimal under iterative decoding
- Nested binary spatially coupled codes suffice for the interference channel
- Not sufficient for compute-and-forward

Quotient rings and p-PAM constellation

Quotient ring

- Principal ideal: $p\mathbb{Z}$ is a principal ideal, e.g., $13\mathbb{Z}$
- Quotient ring: $\mathbb{Z}/p\mathbb{Z}$ is a coset decomposition resulting in a quotient ring
- For any prime p, $\mathbb{Z}_p \triangleq \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$

- $\mathbb{Z}$ is the union of
- $-6 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $-5 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $\vdots$
- $6 + \{\ldots, -13, 0, 13, 26, \ldots\}$

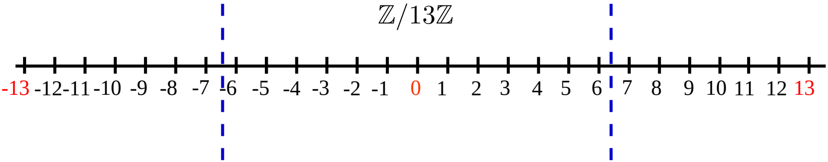


Quotient rings and p-PAM constellation

Quotient ring

- Principal ideal: $p\mathbb{Z}$ is a principal ideal, e.g., $13\mathbb{Z}$
- Quotient ring: $\mathbb{Z}/p\mathbb{Z}$ is a coset decomposition resulting in a quotient ring
- For any prime p, $\mathbb{Z}_p \triangleq \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$

- $\mathbb{Z}$ is the union of
- $-6 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $-5 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $\vdots$
- $6 + \{\ldots, -13, 0, 13, 26, \ldots\}$



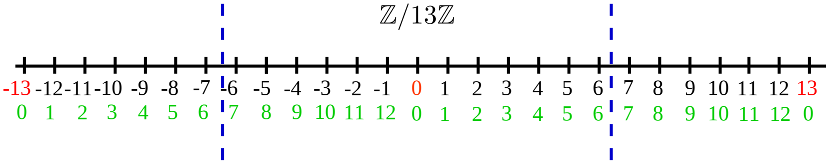
13-PAM is equivalent to $\mathbb{Z}_{13} \triangleq \mathbb{Z}/13\mathbb{Z} \equiv \mathbb{F}_{13}$

Quotient rings and p-PAM constellation

Quotient ring

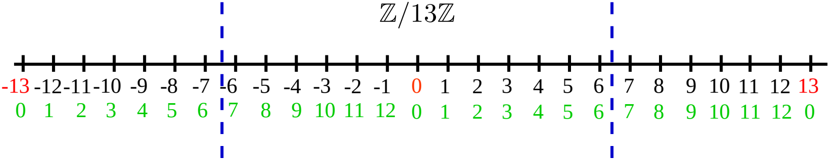
- Principal ideal: $p\mathbb{Z}$ is a principal ideal, e.g., $13\mathbb{Z}$
- Quotient ring: $\mathbb{Z}/p\mathbb{Z}$ is a coset decomposition resulting in a quotient ring
- For any prime p, $\mathbb{Z}_p \triangleq \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$

- $\mathbb{Z}$ is the union of
- $-6 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $-5 + \{\ldots, -13, 0, 13, 26, \ldots\}$
- $\vdots$
- $6 + \{\ldots, -13, 0, 13, 26, \ldots\}$



13-PAM is equivalent to $\mathbb{Z}_{13} \triangleq \mathbb{Z}/13\mathbb{Z} \equiv \mathbb{F}_{13}$

Mappings



Mappings

- Modulation mapping - $\mathcal{M}$ - map from $\mathbb{F}_p$ to $\mathbb{Z}$
- Demodulation mapping - φ - map from $\mathbb{Z}$ to $\mathbb{F}_p$, i.e. $\varphi = z$ mod 13
- Label the elements of $\mathbb{Z}$ with elements from $\mathbb{F}_{13}$ in such a way that $+$, . mod 13 is the same as addition and multiplication in $\mathbb{F}_{13}$

Generalizations

If $\mathcal{R}$ is a ring, ϕ is a prime element in the ring $\boxed{\mathcal{R}/(\phi\mathcal{R}) \cong \mathbb{F}_p}$

$\mathbb{Z}$ is just one ring and $p\mathbb{Z}$ is just one ideal. There are other rings.

Ring homomorphisms

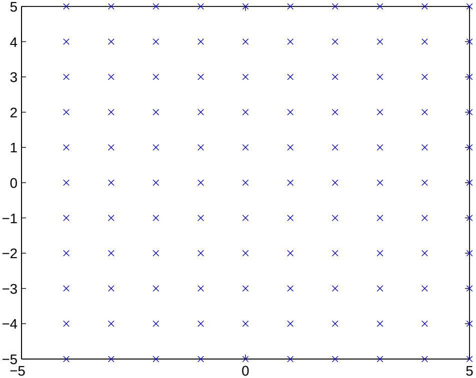
Let $\{\mathcal{R}_1, +, .\}$ and $\{\mathcal{R}_2, \oplus, \odot\}$ be two rings
$\varphi : \mathcal{R}_1 \to \mathcal{R}_2$ is a function that preserves structures

- $\varphi(a + b) = \varphi(a) \oplus \varphi(b), \ \forall a, b \in \mathcal{R}_1$
- $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b), \ \forall a, b \in \mathcal{R}_1$

Some 2-D Examples

Another Example: Gaussian integers $\mathbb{Z}[i]$

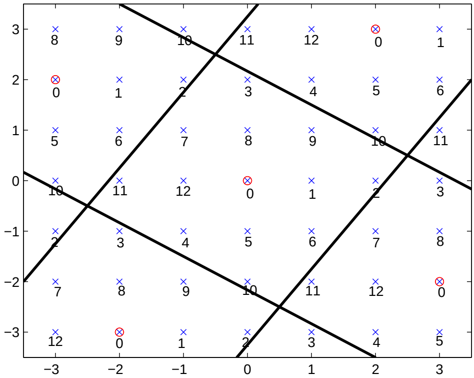
- $\mathbb{Z}[i] = \{a + bj | a, b \in \mathbb{Z}\}$



- $2 + 3i$ is prime in $\mathbb{Z}[i]$ and $|2 + 3i|^2 = 13$
- $\mathbb{Z}[i]/(2 + 3i)\mathbb{Z}[i] \cong \mathbb{F}_{13}$

Another Example: Gaussian integers $\mathbb{Z}[i]$

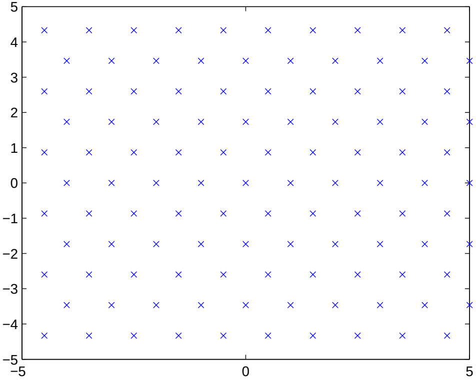
- $\mathbb{Z}[i] = \{a + bj | a, b \in \mathbb{Z}\}$



- $2 + 3i$ is prime in $\mathbb{Z}[i]$ and $|2 + 3i|^2 = 13$
- $\mathbb{Z}[i]/(2 + 3i)\mathbb{Z}[i] \cong \mathbb{F}_{13}$

Another Example: Eisenstein integers $\mathbb{Z}[\omega]$

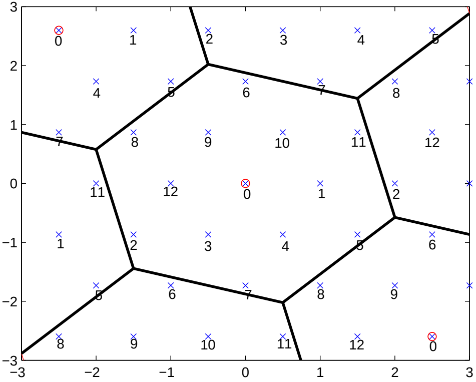
- $\mathbb{Z}[\omega] = \{a + b\omega | \omega = -\frac{1}{2} + j\frac{\sqrt{3}}{2}, a, b \in \mathbb{Z}\}$



- $-1 + 3\omega$ is prime in $\mathbb{Z}[\omega]$ and $|-1 + 3\omega|^2 = 13$
- $\mathbb{Z}[\omega]/(-1 + 3\omega)\mathbb{Z}[\omega] \cong \mathbb{F}_{13}$

Another Example: Eisenstein integers $\mathbb{Z}[\omega]$

- $\mathbb{Z}[\omega] = \{a + b\omega | \omega = -\frac{1}{2} + j\frac{\sqrt{3}}{2}, a, b \in \mathbb{Z}\}$



- $-1 + 3\omega$ is prime in $\mathbb{Z}[\omega]$ and $|-1 + 3\omega|^2 = 13$
- $\mathbb{Z}[\omega]/(-1 + 3\omega)\mathbb{Z}[\omega] \cong \mathbb{F}_{13}$

Now lets deal with the complexity

Introduction to the Chinese Remainder Theorem

Let $p_1, p_2, \ldots, p_L$ be L distinct co-prime integers and $p = p_1.p_2.\ldots.p_L$. 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 $x \in \{0, 1, 2, \ldots, p-1\}$ satisfying this system.

Introduction to the Chinese Remainder Theorem

Let $p_1, p_2, \ldots, p_L$ be L distinct co-prime integers and $p = p_1.p_2.\ldots.p_L$. 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 $x \in \{0, 1, 2, \ldots, p-1\}$ satisfying this system.

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

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

$$\boxed{x = 4}$$

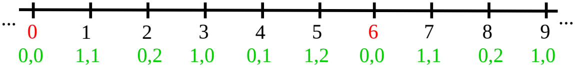
Chinese Remainder Theorem for Rings

Let $p_1, \ldots, p_L$ be distinct primes in $\mathbb{Z}$ and let $p = p_1\ p_2 \ldots p_L$

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

- Consider $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$. Let the isomorphism be

$$\begin{aligned} 0 &\leftrightarrow (0,0), \quad 1 \leftrightarrow (1,1), \quad 2 \leftrightarrow (0,2), \\ 3 &\leftrightarrow (1,0), \quad 4 \leftrightarrow (0,1), \quad 5 \leftrightarrow (1,2), \end{aligned}$$



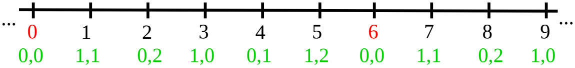
Chinese Remainder Theorem for Rings

Let $p_1, \ldots, p_L$ be distinct primes in $\mathbb{Z}$ and let $p = p_1 \, p_2 \ldots p_L$

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

- Consider $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$. Let the isomorphism be

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

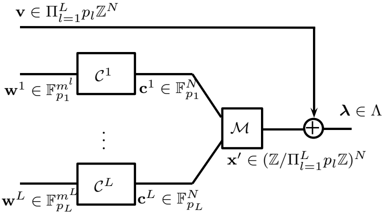


Hence, we have a $\mathcal{M}$ and φ for which add/mult mod 6 is equivalent to two operations - one over $\mathbb{F}_2$ and another over $\mathbb{F}_3$

Proposed Product Construction - Use $\mathbb{Z}$ for Example

Let $p = p_1, \ldots, p_L$ product of distinct primes

$$\mathbb{Z}/\left(p\mathbb{Z}\right) \cong \times_{l=1}^{L} \mathbb{F}_{p_l}$$



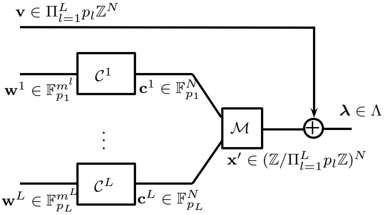
Product construction - L levels

1. Choose $C = C^1 \times \ldots \times C^L$ where $\mathcal{C}^l$ be a linear code over $\mathbb{F}_{p_l}$

Proposed Product Construction - Use $\mathbb{Z}$ for Example

Let $p = p_1, \ldots, p_L$ product of distinct primes

$$\mathbb{Z}/\left(p\mathbb{Z}\right) \cong \times_{l=1}^{L} \mathbb{F}_{p_l}$$



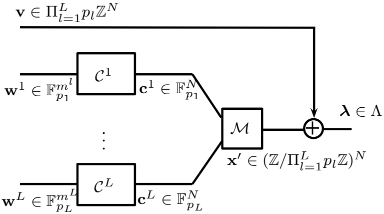
Product construction - L levels

1. Choose $C = C^1 \times \ldots \times C^L$ where $\mathcal{C}^l$ be a linear code over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring homomorphism

Proposed Product Construction - Use $\mathbb{Z}$ for Example

Let $p = p_1, \ldots, p_L$ product of distinct primes

$$\mathbb{Z}/\left(p\mathbb{Z}\right) \cong \times_{l=1}^{L} \mathbb{F}_{p_l}$$



Product construction - L levels

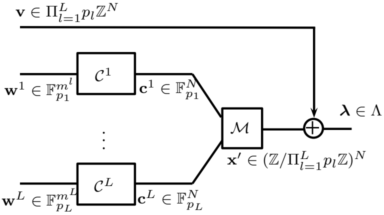
1. Choose $C = C^1 \times \ldots \times C^L$ where $\mathcal{C}^l$ be a linear code over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring homomorphism
3. $\Lambda \triangleq \Lambda^* + p\mathbb{Z}^N$
4. Ring homomorphism: $\varphi \triangleq \mathcal{M}^{-1} \circ \bmod p\mathbb{Z}$

Works for other rings such as $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

Proposed Product Construction - Use $\mathbb{Z}$ for Example

Let $p = p_1, \ldots, p_L$ product of distinct primes

$$\mathbb{Z}/\left(p\mathbb{Z}\right) \cong \times_{l=1}^{L} \mathbb{F}_{p_l}$$



Product construction - L levels

1. Choose $C = C^1 \times \ldots \times C^L$ where $\mathcal{C}^l$ be a linear code over $\mathbb{F}_{p_l}$
2. $\Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L)$ where $\mathcal{M}$ is ring homomorphism
3. $\Lambda \triangleq \Lambda^* + p\mathbb{Z}^N$
4. Ring homomorphism: $\varphi \triangleq \mathcal{M}^{-1} \circ \bmod p\mathbb{Z}$

Works for other rings such as $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

Reduce to Construction A when $L = 1$

Properties of construction-π_A

Theorem 1

The proposed construction results in a lattice

Proof.

Construction-A only hinges on the mapping. Chinese remainder theorem shows that such a mapping exists. □

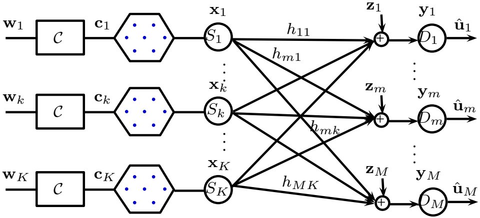
Theorem 2

There exists a sequence of proposed multilevel lattices that are Poltyrev-good

Theorem 3

There exists a sequence of proposed multilevel lattices MSE quantization-good

Example of Multistage CF

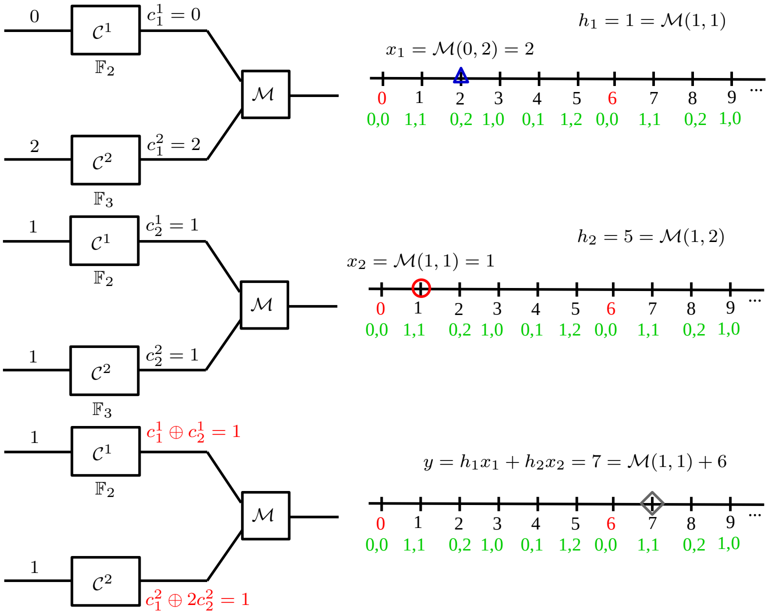


$$
\begin{aligned}
y_3 &= x_1 + 5x_2 + h_{33}x_3 + z_3 \\
&= \boxed{x_1 + 5x_2} + z_{eq,3}
\end{aligned}
$$

- Consider $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$. Same isomorphism and codes.

$$
\begin{aligned}
&0 \leftrightarrow (0,0), \quad 1 \leftrightarrow (1,1), \quad 2 \leftrightarrow (0,2), \\
&3 \leftrightarrow (1,0), \quad 4 \leftrightarrow (0,1), \quad 5 \leftrightarrow (1,2),
\end{aligned}
$$

Example of Multistage CF

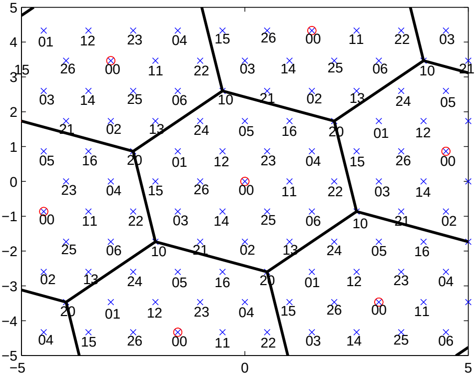


Example from $\mathbb{Z}[\omega]$

$$\phi_1 = 3 + 2\omega, \phi_2 = 1 + 2\omega, \phi = \phi_1\phi_2, \mathbb{Z}[\omega]/\phi\mathbb{Z}[\omega] \cong \mathbb{F}_3 \times \mathbb{F}_7$$

$$x_1 = 1 \Leftrightarrow \mathbf{c}_1 = (1,1), \quad x_2 = -1 \Leftrightarrow \mathbf{c}_2 = (2,6)$$

channel coeffs: $h_1 = 1$, $h_2 = \omega \Leftrightarrow$ Want to decode: $1 \cdot x_1 + \omega \cdot x_2 = 1 - \omega$

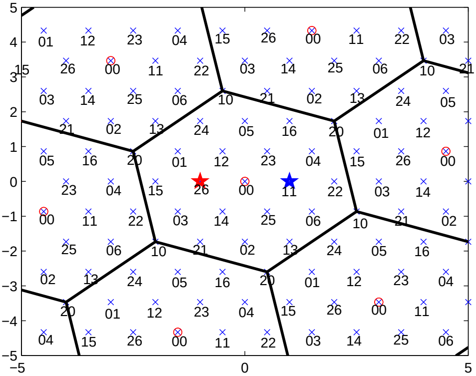


Example from $\mathbb{Z}[\omega]$

$$\phi_1 = 3 + 2\omega, \phi_2 = 1 + 2\omega, \phi = \phi_1\phi_2, \mathbb{Z}[\omega]/\phi\mathbb{Z}[\omega] \cong \mathbb{F}_3 \times \mathbb{F}_7$$

$$x_1 = 1 \Leftrightarrow \mathbf{c}_1 = (1,1), \quad x_2 = -1 \Leftrightarrow \mathbf{c}_2 = (2,6)$$

channel coeffs: $h_1 = 1$, $h_2 = \omega \Leftrightarrow$ Want to decode: $1 \cdot x_1 + \omega \cdot x_2 = 1 - \omega$



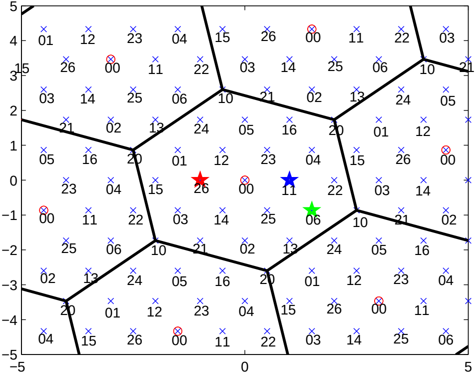
- $a_1\mathbf{c}_1 \oplus a_2\mathbf{c}_2 = (1,1) \odot (1,1) \oplus (1,2) \odot (2,6) = (1,1) \oplus (2,5) = (0,6)$
- Equivalent to decoding $[\mathbf{c}_1^1 \oplus \mathbf{c}_2^1 \;\; \mathbf{c}_1^2 \oplus 2 \cdot \mathbf{c}_2^2]$

Example from $\mathbb{Z}[\omega]$

$$\phi_1 = 3 + 2\omega, \phi_2 = 1 + 2\omega, \phi = \phi_1\phi_2, \mathbb{Z}[\omega]/\phi\mathbb{Z}[\omega] \cong \mathbb{F}_3 \times \mathbb{F}_7$$

$$x_1 = 1 \Leftrightarrow \mathbf{c}_1 = (1, 1), \quad x_2 = -1 \Leftrightarrow \mathbf{c}_2 = (2, 6)$$

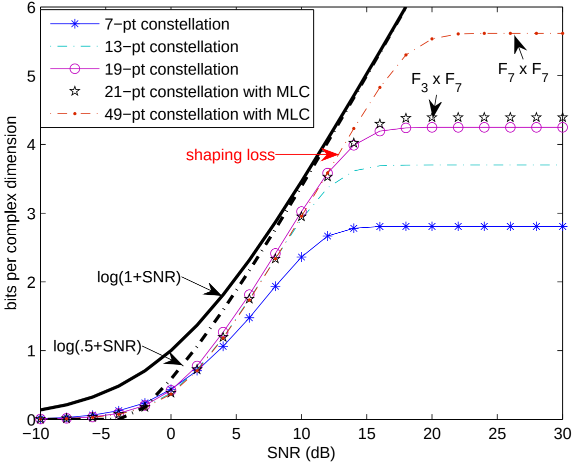
channel coeffs: $h_1 = 1$, $h_2 = \omega \Leftrightarrow$ Want to decode: $1 \cdot x_1 + \omega \cdot x_2 = 1 - \omega$



- $a_1\mathbf{c}_1 \oplus a_2\mathbf{c}_2 = (1, 1) \odot (1, 1) \oplus (1, 2) \odot (2, 6) = (1, 1) \oplus (2, 5) = (0, 6)$
- Equivalent to decoding $[\mathbf{c}_1^1 \oplus \mathbf{c}_2^1 \ \ \mathbf{c}_1^2 \oplus 2 \cdot \mathbf{c}_2^2]$

Numerical Results - 2 TX and 1 RX

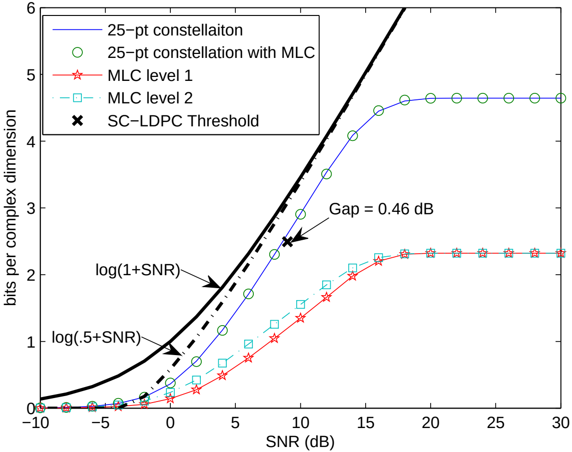
$$h_1 = h_2 = 1.$$



Numerical and Simulation Results - 2 TX and 1 RX

$$\phi = 5,\ h_1 = h_2 = 1.$$

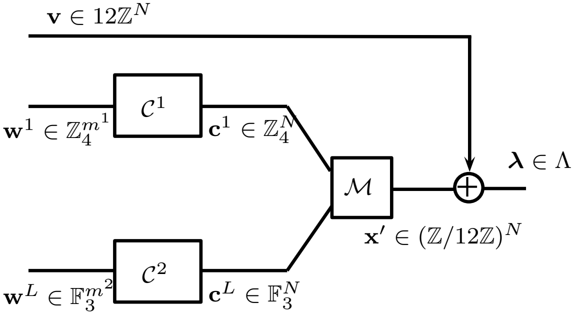
$\times$: Simulated by $(3, 6, 64, 10000)$ SC-LDPC code



When p is not a product of primes..

EX: $p = 12 = 4 \times 3$

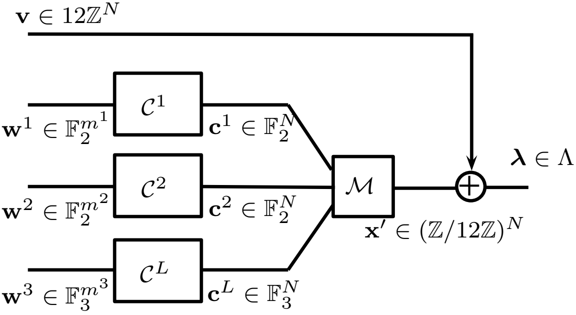
$$\begin{aligned} \mathbb{Z}_{12} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{F}_3 \\ \mathbb{Z}_{12} &\ncong \mathbb{F}_4 \times \mathbb{F}_3 \end{aligned}$$



When p is not a product of primes..

EX: $p = 12 = 4 \times 3$

$$
\begin{aligned}
\mathbb{Z}_{12} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{F}_3 \\
\mathbb{Z}_{12} &\ncong \mathbb{F}_4 \times \mathbb{F}_3
\end{aligned}
$$



$\mathcal{C}^1 \subset \mathcal{C}^2$

Primes to Powers of 2

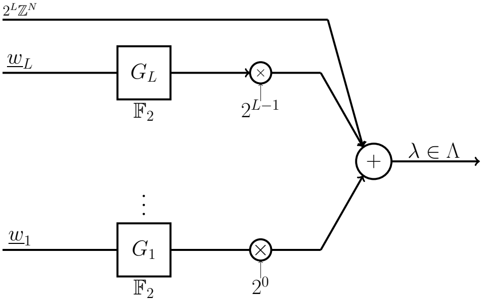
Mathematicians like prime numbers, Engineers like powers of two

- Emanuele Viterbo

Construction D with L levels

- Barnes and Sloane '83, Forney, Chung and Trott '00, Yan, Ling, Wu ' 13

$$G = \left[\begin{array}{ccc} \cdots & g_L & \cdots \\ \cdots & \vdots & \cdots \\ \hline \cdots & g_{k_2} & \cdots \\ \cdots & \vdots & \cdots \\ \hline \cdots & g_{k_1} & \cdots \\ \cdots & \vdots & \cdots \\ \cdots & g_2 & \cdots \\ \cdots & g_1 & \cdots \end{array}\right]$$



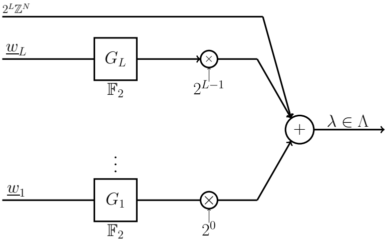
1. Choose $G_1 \subseteq \ldots \subseteq G_L$ where G_l is a gen matrix of a code over $\mathbb{F}_2$.
2. Lattice built using nested codes obtained by nested generator matrices:

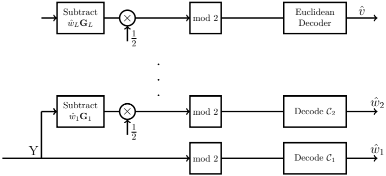
$$\Lambda = \left\{\underline{w}_1\mathbf{G}_1 + 2\underline{w}_2\mathbf{G}_2 \ldots + 2^{L-1}\underline{w}_{L-1}\mathbf{G}_{L-1} + 2^L\mathbb{Z}^N : w_{j,i} \in \{0,1\}\right\}$$

3. $(\underline{w}_1\mathbf{G}_1)$ mod 2 $= \underline{w}_1 \odot \mathbf{G}_1$

Multi-Level Decoding(Successive Decoding)

- $\underline{y} = \underline{w}_1\mathbf{G}_1 + 2\underline{w}_2\mathbf{G}_2 \ldots + 2^{L-1}\underline{w}_{L-1}\mathbf{G}_{L-1} + 2^L\mathbb{Z}^N + \underline{n}$
- $\underline{y}$ mod 2 $= (\underline{w}_1\mathbf{G}_1 + \underline{n})$ mod 2 $=$ $\boxed{\underline{w}_1 \odot \mathbf{G}_1 + \underline{n}}$ mod 2
- Decode $\underline{w}_1$, reconstruct $\underline{w}_1\mathbf{G}_1$ and subtract from $\underline{y}$





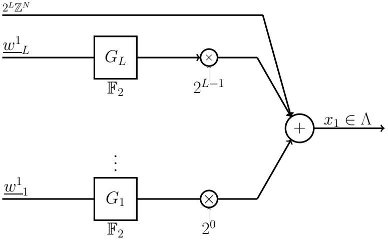
Decoding Sums - Symmetric Interference Channel(SIC)

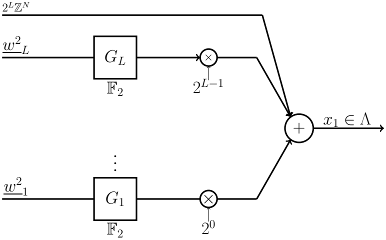
- 2-level code for each user

$$\begin{aligned}\mathbf{x}_1 + \mathbf{x}_2 &= (\underline{w}_1^1 + \underline{w}_1^2)\mathbf{G}_1 + 2(\underline{w}_2^1 + \underline{w}_2^2)\mathbf{G}_2 + 4\mathbf{k}_{12} \\ &= (\underline{w}_1^1 \oplus \underline{w}_1^2 + 2\underline{c}_1)\mathbf{G}_1 + 2(\underline{w}_2^1 \oplus \underline{w}_2^2)\mathbf{G}_2 + 4\underline{c}_2\mathbf{k}_{23} \\ &= (\underline{w}_1^1 \oplus \underline{w}_1^2)\mathbf{G}_1 + 2(\underline{c}_1 + \underline{w}_2^1 + \underline{w}_2^2)\mathbf{G}_2 + 4\underline{c'}_2\mathbf{k}_{23}\end{aligned}$$

where the carry overs are

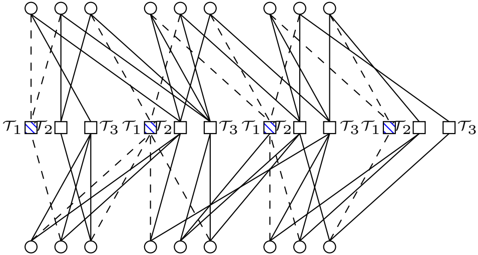
$$\begin{aligned}2\underline{c}_1 + \underline{w}_1^1 \oplus \underline{w}_1^2 &= \left(\underline{w}_1^1 + \underline{w}_1^2\right), \\ 2\underline{c}_2 + \underline{c}_1 \oplus \underline{w}_2^1 \oplus \underline{w}_2^2 &= \left(\underline{c}_1 + \underline{w}_2^1 + \underline{w}_2^2\right)\end{aligned}$$



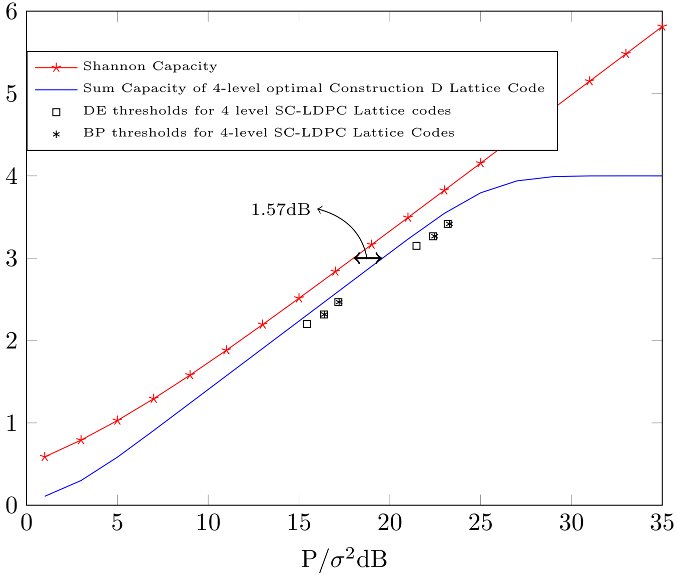


Proposed Nested Spatially-Coupled LDPC Ensemble (Regular here)

1. Begin with a (d_v^1, d_c) SC LDPC code
2. Group check nodes into type $\mathcal{T}_k$, $k \in \{1, \ldots, d_v^1\}$
3. Remove all check nodes of type $\mathcal{T}_1, \ldots, \mathcal{T}_{d_v^1 - d_v^2}$
4. Results in a sub-code that is a (d_v^2, d_c) SC LDPC code



Achievable Information Rates



Concluding Remarks

- Multilevel constructions - efficient ways to decode integer combinations
- Multilevel construction are provably good
- Multilevel with different primes - no need for nesting
- For powers of 2, codes need to be nested
- These constructions are provably good under message passing decoding
- Nothing more than non-binary LDPC codes over small fields are required