

Lattice Index Coding

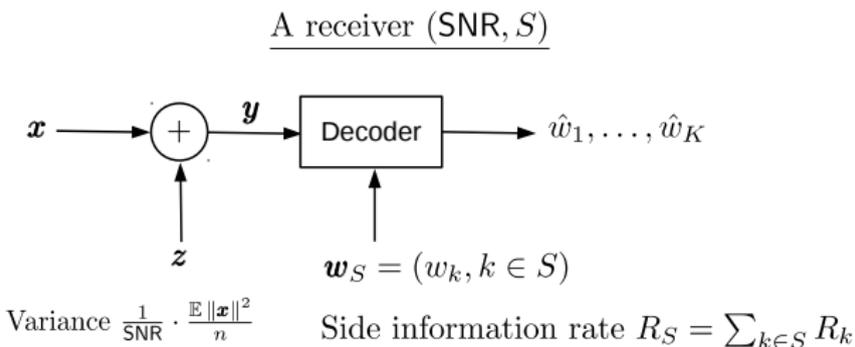
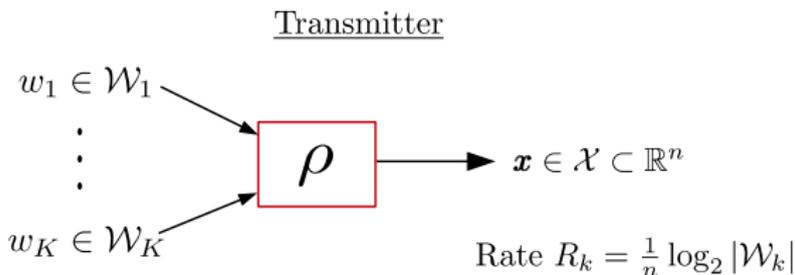
Part III - Constructing Codes

Emanuele Viterbo

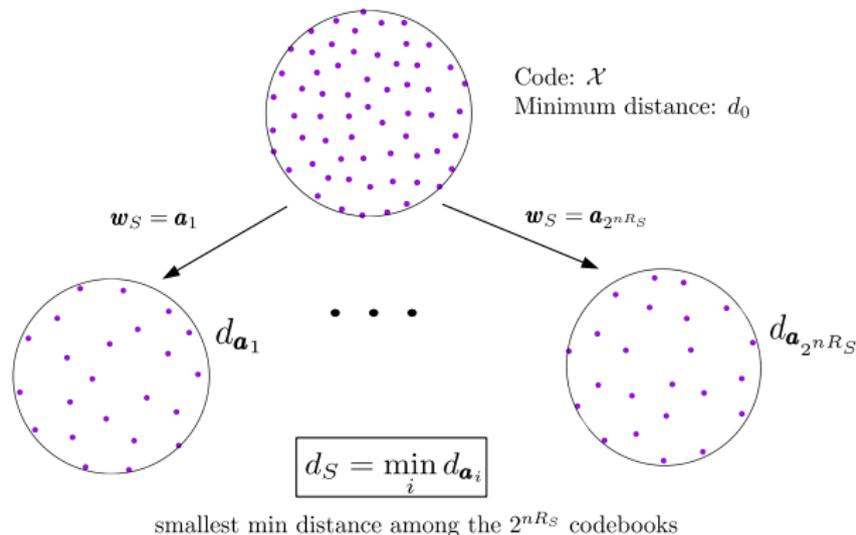
European School of Information Theory
4 April 2016, Gothenburg

Recap: Channel Model

Broadcast (w_1, \dots, w_K) to multiple receivers $\{(\text{SNR}, S)\}$ where $S \subset \{1, \dots, K\}$ denotes the available side information



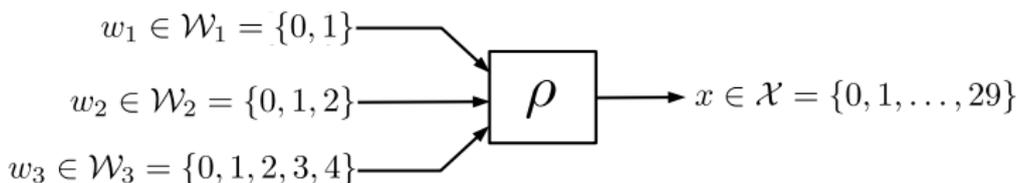
Recap: Decoding and Side Information Gain



$$\text{Side Information Gain } \Gamma(\mathcal{X}) = \min_{S \subset \{1, \dots, K\}} \frac{10 \log_{10} \left(\frac{d_S^2}{d_0^2} \right)}{R_S} \text{ dB/b/dim}$$

Design Objective: maximize d_0 and $\Gamma(\mathcal{X})$

Algebraic Construction: Main Idea



- Label 30-PAM with elements of the ring $\mathbb{Z}_{30} = \{0, 1, \dots, 29\}$.
 - ▶ Addition and multiplication in \mathbb{Z}_{30} are performed modulo 30.
- Encode messages to $\mathcal{X} = \mathbb{Z}_{30}$ using

$$x = \rho(w_1, w_2, w_3) = 15w_1 + 10w_2 + 6w_3 \pmod{30}.$$

- Chinese remainder theorem $\Rightarrow \rho$ is bijective.
- Dimension of the codebook is $n = 1$.
- $R_1 = 1$, $R_2 = \log_2 3$, $R_3 = \log_2 5$ b/dim.

$$x = 15w_1 + 10w_2 + 6w_3 \pmod{30}$$

$$S = \{1, 2\}$$

$$\mathcal{X}_{a_S} = 6w_3 + \text{constant}$$



$$S = \{1\}$$

$$\mathcal{X}_{a_S} = 10w_2 + 6w_3 + \text{constant}$$



$$S = \{1, 3\}$$

$$\mathcal{X}_{a_S} = 10w_2 + \text{constant}$$



$$S = \{2\}$$

$$\mathcal{X}_{a_S} = 15w_1 + 6w_3 + \text{constant}$$



$$S = \{2, 3\}$$

$$\mathcal{X}_{a_S} = 15w_1 + \text{constant}$$



$$S = \{3\}$$

$$\mathcal{X}_{a_S} = 15w_1 + 10w_2 + \text{constant}$$



$$S = \emptyset$$

$$\mathcal{X}_{a_S} = \mathcal{X} = \{0, 1, \dots, 29\}$$



$$d_S = 2^{R_S}$$

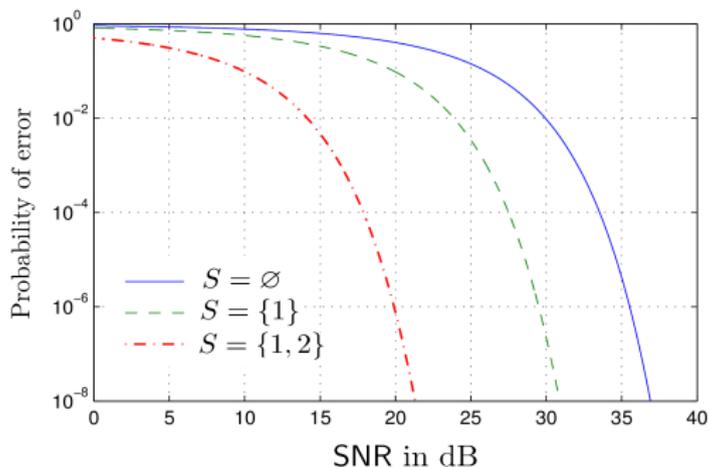
Side information gain

- The code guarantees: $d_S = 2^{R_S}$ for all $\emptyset \subsetneq S \subsetneq \{1, 2, 3\}$
 - ▶ Min distance improves with the amount of available side information
- Side information gain

$$\Gamma(\mathcal{X}) = \min_S \frac{10 \log_{10} (d_S^2/d_0^2)}{R_S} = \min_S \frac{10 \log_{10} (d_S^2)}{\log_2 d_S} = 20 \log_{10} 2 \\ \approx 6 \text{ dB/b/dim.}$$

- Uniform Side Information Gain:
Identical normalized distance gain for all receivers

$$\frac{10 \log_{10} (d_S^2/d_0^2)}{R_S} = 20 \log_{10} 2 \approx 6 \text{ for all } S \subset \{1, 2, 3\}$$



SNR gain over $S = \emptyset$ at $P_e = 10^{-4}$

S	Actual gain	Predicted $\Gamma \times R_S$ dB
$\{1\}$	6	6
$\{1, 2\}$	15.6	15.5

Algebraic Construction over \mathbb{Z}

In order to encode K messages:

- Choose K relatively prime integers: $M_1, \dots, M_K \in \mathbb{Z}$.
- The message alphabets are $\mathcal{W}_1 = \mathbb{Z}/M_1\mathbb{Z}, \dots, \mathcal{W}_K = \mathbb{Z}/M_K\mathbb{Z}$.
- Encode messages to M -PAM, where $M = \prod_{k=1}^K M_k$:

$$\rho(w_1, \dots, w_K) = \frac{M}{M_1} w_1 + \dots + \frac{M}{M_K} w_K \pmod{M}.$$

- This map corresponds to the Chinese remainder theorem:

$$\mathbb{Z}/M_1\mathbb{Z} \times \dots \times \mathbb{Z}/M_K\mathbb{Z} \rightarrow \mathbb{Z}/M\mathbb{Z}.$$

- Rate $R_k = \log_2 M_k$ b/dim.

Algebraic Construction over \mathbb{Z}

Distance with no side information

- $d_0 = \min$ distance of M -PAM $\mathbb{Z}/M\mathbb{Z} = 1$

Distance with side information configuration S

- Receiver knows $w_k = a_k, k \in S$
- Expurgated codebook consists of the points

$$x = \sum_{k \in S} \frac{M}{M_k} a_k + \sum_{k \notin S} \frac{M}{M_k} w_k \pmod{M}, \text{ where } w_k \text{ are unknown integers}$$

- Difference between codewords $\Delta x = \sum_{k \notin S} \frac{M}{M_k} \Delta w_k \pmod{M}$
- Minimum distance d_S

$$\min |\Delta x| = \min \left| \sum_{k \notin S} \frac{M}{M_k} \Delta w_k \right| = \gcd \left(\frac{M}{M_k}, k \notin S \right) = \prod_{k \in S} M_k$$

Algebraic Construction over \mathbb{Z}

Side Information Gain

- Distance with side information

$$d_S = \prod_{k \in S} M_k = \prod_{k \in S} 2^{R_k} = 2^{\sum_{k \in S} R_k} = 2^{R_S}$$

- Side information gain

$$\Gamma = \min_S \frac{10 \log_{10} \left(\frac{d_S^2}{d_0^2} \right)}{R_S} \approx 6 \text{ dB/b/dim}$$

Construction over $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

- Choose K relatively-prime numbers $M_1, \dots, M_K \in \mathbb{D}$
- Message alphabets: $\mathcal{W}_1 = \mathbb{D}/M_1\mathbb{D}, \dots, \mathcal{W}_K = \mathbb{D}/M_K\mathbb{D}$
- Rate: $R_k = \log_2 |M_k|$ b/dim
- Constellation: $\mathcal{X} = \mathbb{D}/M\mathbb{D}$, where $M = M_1 M_2 \cdots M_K$
- Encoding: Using Chinese remainder theorem

$$\rho(w_1, \dots, w_K) = \frac{M}{M_1}w_1 + \cdots + \frac{M}{M_K}w_k \pmod{M\mathbb{D}}$$

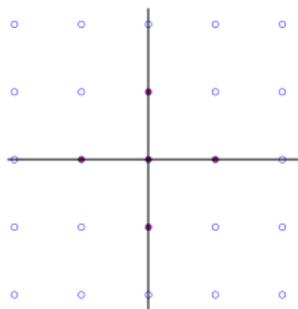
- Minimum distance:

$$d_0 = d_{\min}(\mathbb{D}) = 1 \quad d_S = \left| \gcd \left(\frac{M}{M_k}, k \notin S \right) \right| = \left| \prod_{k \in S} M_k \right| = 2^{R_S}$$

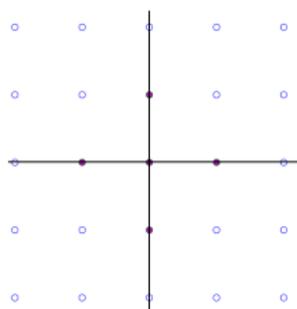
- Side information gain: $\Gamma = 20 \log_{10} 2 \approx 6$ dB/b/dim

$$\mathbb{D} = \mathbb{Z}[i], K = 2, (M_1, M_2) = (1 + 2i, 1 - 2i), M = 5$$

$$w_1 \in \mathbb{Z}[i]/(1 + 2i)\mathbb{Z}[i] \cong \mathbb{F}_5$$

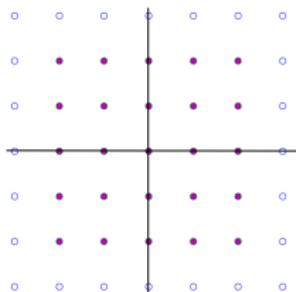


$$w_2 \in \mathbb{Z}[i]/(1 - 2i)\mathbb{Z}[i] \cong \mathbb{F}_5$$



$$x = w_1 \frac{M}{M_1} + w_2 \frac{M}{M_2} \pmod{M\mathbb{D}}$$

$$x = w_1(1 - 2i) + w_2(1 + 2i) \pmod{5\mathbb{Z}[i]}$$



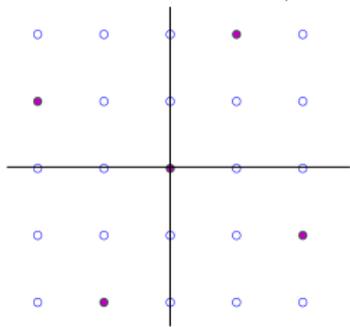
$$\begin{aligned} 5 &= (1 + 2i)(1 - 2i) \\ \gcd(1 + 2i, 1 - 2i) &= 1 \end{aligned}$$

$$\begin{aligned} \mathcal{X} &= \mathbb{Z}[i]/5\mathbb{Z}[i] \\ d_0 &= d_{\min}(\mathbb{Z}[i]) = 1 \end{aligned}$$

$$x = w_1(1 - 2i) + w_2(1 + 2i) \bmod 5\mathbb{Z}[i]$$

$$S = \{1\}$$

$$x = \left(w_2(1 + 2i) + \text{constant} \right) \bmod 5\mathbb{Z}[i]$$

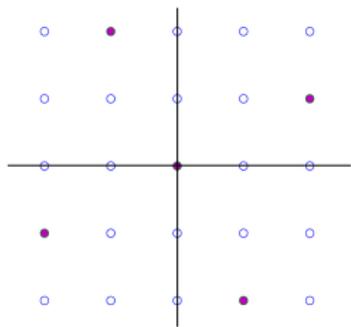


$$d_S = |1 + 2i| = \sqrt{5}$$

$$R_S = \frac{1}{2} \log_2 5$$

$$S = \{2\}$$

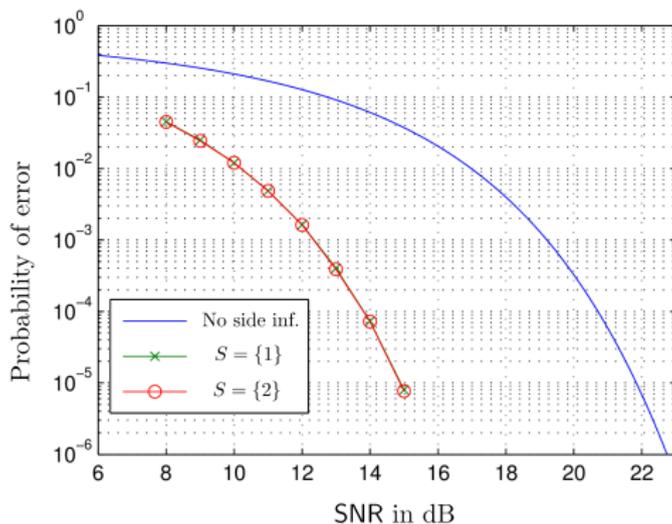
$$x = \left(w_1(1 - 2i) + \text{constant} \right) \bmod 5\mathbb{Z}[i]$$



$$d_S = |1 - 2i| = \sqrt{5}$$

$$R_S = \frac{1}{2} \log_2 5$$

$$\Gamma = \min_{S=\{1\},\{2\}} \frac{10 \log_{10}(d_S^2/d_0^2)}{R_S} = \frac{10 \log_{10} 5}{\frac{1}{2} \log_2 5} \approx 6 \text{ dB/b/dim}$$

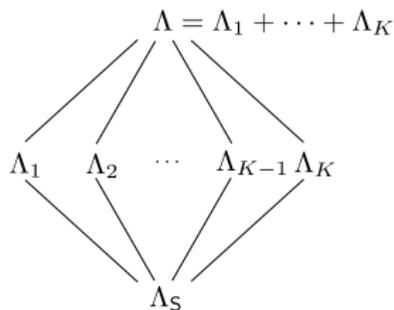


SNR gain over $S = \emptyset$ at $P_e = 10^{-5}$

S	Actual gain	Predicted $\Gamma \times R_S$ dB
$\{1\}$	6.9	6.9
$\{2\}$	6.9	6.9

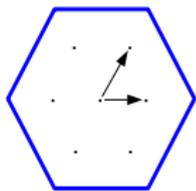
How to construct codes in higher dimensions?

Use a family of lattices



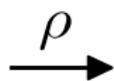
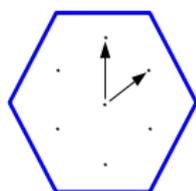
Lattice index code:

$$\mathcal{X}_1 = \Lambda_1 / \Lambda_S$$

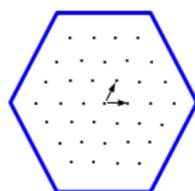


+ \dots +
(Direct sum)

$$\mathcal{X}_K = \Lambda_K / \Lambda_S$$



$$\mathcal{X} = \Lambda / \Lambda_S$$



Lattice index codes

Definition

A *lattice index code* consists of nested lattice codes $\Lambda_1/\Lambda_s, \dots, \Lambda_K/\Lambda_s$ such that the encoding map $\rho : \Lambda_1/\Lambda_s \times \dots \times \Lambda_K/\Lambda_s \rightarrow \Lambda/\Lambda_s$,

$$\rho(\mathbf{x}_1, \dots, \mathbf{x}_K) = (\mathbf{x}_1 + \dots + \mathbf{x}_K) \bmod \Lambda_s,$$

is one-to-one.

- $\Lambda_1/\Lambda_s, \dots, \Lambda_K/\Lambda_s$ are subgroups of Λ/Λ_s (under addition mod Λ_s)
- One-to-one map ensures unique decodability and implies

$$\Lambda_1/\Lambda_s \times \dots \times \Lambda_K/\Lambda_s \cong \Lambda/\Lambda_s \text{ (as groups)}$$

- Rate $R_k = \frac{1}{n} \log_2 \frac{\text{Vol}(\Lambda_s)}{\text{Vol}(\Lambda_k)}$
- Minimum distance

$$d_0 = d_{\min}(\Lambda) \quad d_S = d_{\min} \left(\sum_{k \notin S} \Lambda_k \right)$$

Properties

Effective codebook with side information configuration $S \subset \{1, \dots, K\}$

- ..is a translate of the lattice code $(\sum_{k \notin S} \Lambda_k) / \Lambda_s$
- Coding gain is the center density of the coding lattice $\sum_{k \notin S} \Lambda_k$

$$\delta \left(\sum_{k \notin S} \Lambda_k \right) = \frac{(r_{\text{pack}}(\sum_{k \notin S} \Lambda_k))^n}{\text{Vol}(\sum_{k \notin S} \Lambda_k)}$$

- When $S = \emptyset$, i.e., no side information, coding gain = $\delta(\Lambda)$

Distance gain due to side information

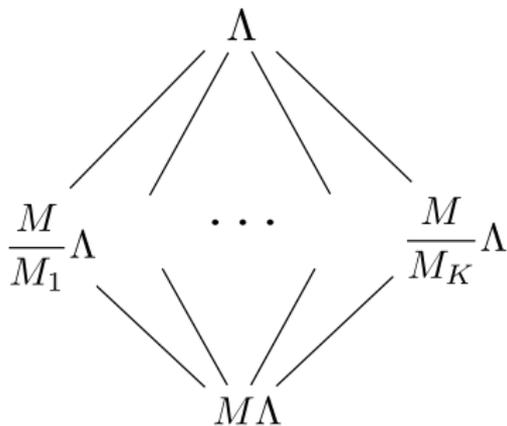
$$\frac{d_S}{d_0} = 2^{R_S} \times \left[\frac{\delta(\sum_{k \notin S} \Lambda_k)}{\delta(\Lambda)} \right]^{\frac{1}{n}}$$

Lemma

If Λ is a densest lattice in \mathbb{R}^n then $\Gamma(\Lambda/\Lambda_s) \leq 20 \log_{10} 2 \approx 6 \text{ dB/b/dim}$

Construction using Chinese Remainder Theorem

- Let $\mathbb{D} = \mathbb{Z}, \mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$ and Λ be any \mathbb{D} -lattice
 - ▶ Λ can be a known lattice with large coding gain
- Let $M_1, \dots, M_K \in \mathbb{D}$ be relatively prime, $M = \prod_{k=1}^K M_k$
- Scale Λ by $\frac{M}{M_1}, \dots, \frac{M}{M_K}$ to generate a family of lattices.



- Rate $R_k = \log_2 |M_k|$ b/dim.
- $\delta(\sum_{k \notin S} \Lambda_k) = \delta(\Lambda)$ for any S
- $d_0 = d_{\min}(\Lambda)$
- $\frac{d_S}{d_0} = 2^{R_S}$ for any S
- $\Gamma \approx 6$ dB/b/dim

Further Algebraic Constructions

Over general algebraic number fields (Huang, ISIT'15)

- Use the ring of integers $\mathcal{O}_{\mathbb{K}}$ of an algebraic number field \mathbb{K}
- The elements of $\mathcal{O}_{\mathbb{K}}$ can be embedded into a lattice
- Construct lattice codes using Chinese remainder theorem in $\mathcal{O}_{\mathbb{K}}$
- All the K messages can be allowed to take values from the same finite field
- If \mathbb{K} is totally real: diversity gain in Rayleigh fading channel
- Both minimum Euclidean distance and minimum product distance improve with side information

Over Hurwitz quaternionic integers

- Non-commutative Euclidean domain that is geometrically equivalent to D_4^* lattice
- Corresponding lattice code has a larger coding gain than $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ constructions and provides more options for encoding rates

Summary of algebraic construction

- Using nested lattice codes for physical-layer index coding
- Algebraic labelling of codewords using Chinese remainder theorem
- Side information gain of at least 6 dB/b/dim
- Effective codebook at the receivers are also nested lattice codes
 - ▶ Can employ lattice decoding at the receivers

However..

- Decoding complexity is high for large dimensions
- Message sizes are not powers of 2

In the next section..

- We design a concatenated scheme that can be decoded with low-complexity iterative detection
- The modulation scheme (inner code) will encode integer number of bits while ensuring side information gain

Index Coding using Multidimensional PAM

- **Message alphabet:**

$$\mathcal{W}_1 = \dots = \mathcal{W}_K = \mathbb{Z}/M\mathbb{Z} \triangleq \mathbb{Z}_M$$

- **Codebook:** K -tuples over \mathbb{Z}_M

$$\mathcal{X} = \mathbb{Z}_M \times \dots \times \mathbb{Z}_M = \mathbb{Z}_M^K$$

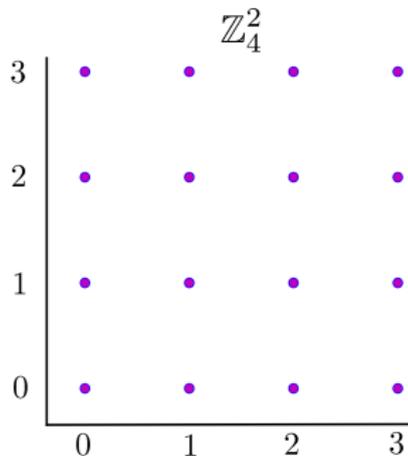
- Embed \mathcal{X} into \mathbb{R}^K using natural map

- Use a linear encoder to map messages to codeword

$$\begin{aligned} \mathcal{W}_1 \times \dots \times \mathcal{W}_K &\rightarrow \mathcal{X} \\ \mathbb{Z}_M^K &\rightarrow \mathbb{Z}_M^K \end{aligned}$$

- Generate codeword \mathbf{x} as linear combination of $\mathbf{c}_1, \dots, \mathbf{c}_K \in \mathbb{Z}_M^K$:

$$\mathbf{x} = \rho(w_1, \dots, w_K) = \sum_{k=1}^K w_k \mathbf{c}_k \pmod{M}.$$



Properties

- Code is fully characterized by the $K \times K$ generating matrix over \mathbb{Z}_M

$$\mathbf{C} = [\mathbf{c}_1 \ \mathbf{c}_2 \ \cdots \ \mathbf{c}_K]$$

- Code length $n =$ number of messages K .
- All messages are encoded at the same rate

$$R_1 = \cdots = R_K = \frac{1}{K} \log_2 M \text{ b/dim.}$$

- ρ is bijective $\Leftrightarrow \mathbf{C}$ is invertible, i.e., $\det(\mathbf{C})$ is a unit in \mathbb{Z}_M
- Minimum distance with no side information $d_0 = d_{\min}(\mathbb{Z}_M^K) = 1$

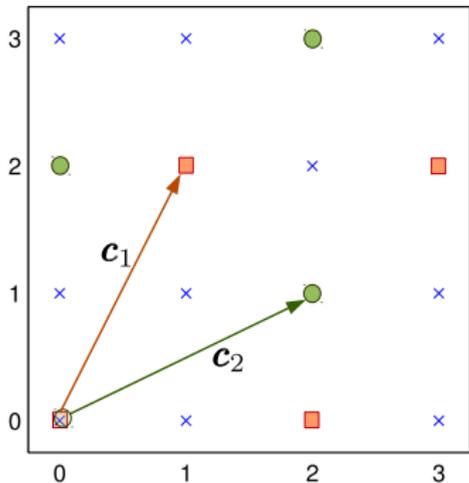
Properties

- Using linearity property, $d_S = d_{\min}(\mathcal{C}_S)$, where

$$\mathcal{C}_S = \left\{ \sum_{k \notin S} w_k \mathbf{c}_k \mid w_k \in \mathbb{Z}_M, k \notin S \right\} \text{ is a } \mathbb{Z}_M\text{-linear code}$$

- d_S can be computed using shortest-vector algorithm for lattices
- Therefore $\Gamma = \min_S \frac{10 \log_{10}(d_S^2/d_0^2)}{R_S}$ can be efficiently computed using numerical techniques

Example: 16-QAM index code using \mathbb{Z}_4



- $\mathbf{C} = (\mathbf{c}_1 \ \mathbf{c}_2) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

- $\det(\mathbf{C}) = -3 \bmod 4 = 1 \in U(\mathbb{Z}_4)$.

- $S = \{1\}$:

$$\mathcal{C}_S = \{w_2 \mathbf{c}_2 \mid w_2 \in \mathbb{Z}_4\},$$

$$d_S = 2.$$

- $S = \{2\}$:

$$\mathcal{C}_S = \{w_1 \mathbf{c}_1 \mid w_1 \in \mathbb{Z}_4\},$$

$$d_S = 2.$$

$$\Gamma \approx 6 \text{ dB/b/dim}$$

Computer Search for Good Codes

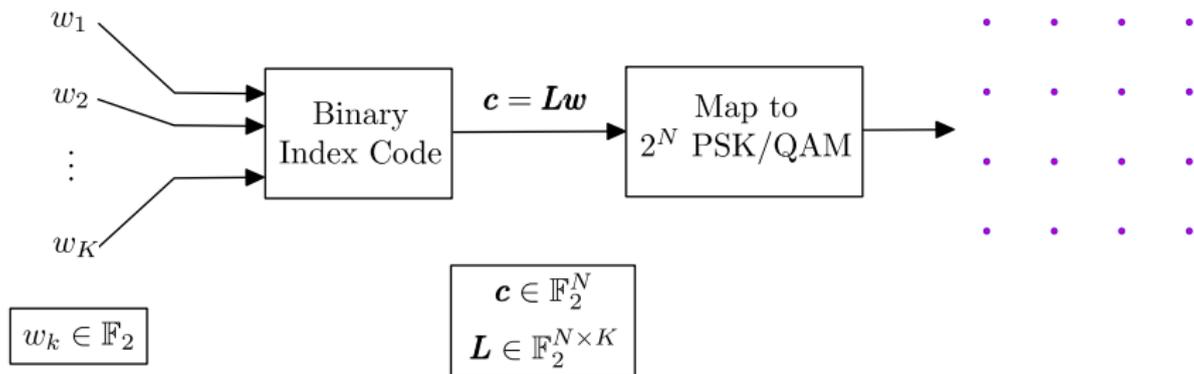
- We restrict search space to codes with circulant \mathbf{C} matrix.
- Table gives the first column of \mathbf{C} and Γ for the best codes.

M	$K = n$			
	2	3	4	5
4	$(1, 2)^\top$ 6.02	$(1, 2, 2)^\top$ 4.52	$(1, 1, 3, 0)^\top$ 3.01	$(1, 2, 1, 3, 0)^\top$ 3.76
8	$(1, 2)^\top$ 4.65	$(1, 2, 0)^\top$ 3.49	$(1, 0, 3, 3)^\top$ 4.01	$(1, 7, 2, 2, 5)^\top$ 4.70
16	$(1, 12)^\top$ 6.02	$(1, 2, 10)^\top$ 5.24	$(1, 4, 10, 8)^\top$ 5.57	$(1, 14, 11, 12, 5)^\top$ 5.28
32	$(1, 6)^\top$ 5.85	$(1, 22, 14)^\top$ 5.73	$(1, 10, 14, 2)^\top$ 5.80	$(1, 24, 27, 15, 26)^\top$ 5.77
64	$(1, 36)^\top$ 6.04	$(1, 38, 60)^\top$ 5.73	$(1, 38, 20, 30)^\top$ 5.85	$(1, 16, 18, 55, 21)^\top$ 5.82

Modulation scheme ensures large side information gain

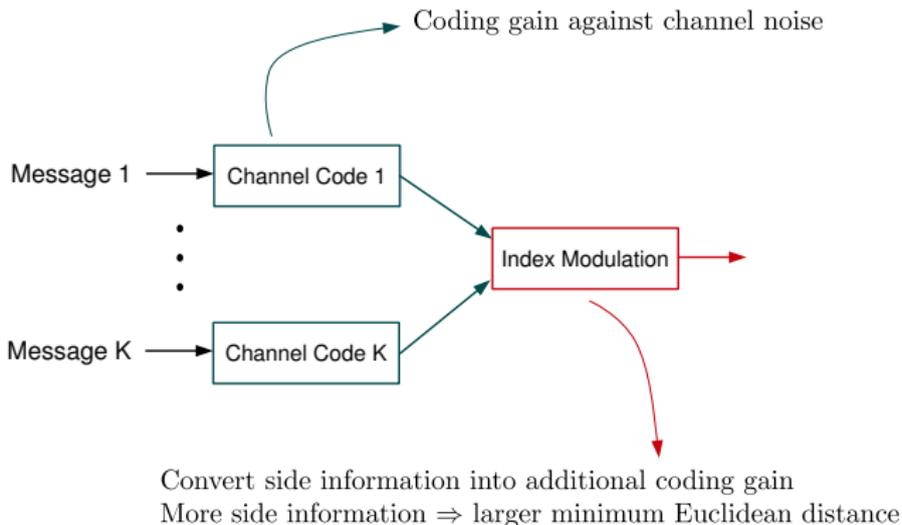
Further Modulation Schemes for Index Coding (Mahesh & Rajan, arXiv:1603.03152)

Multiple receivers with general message demands



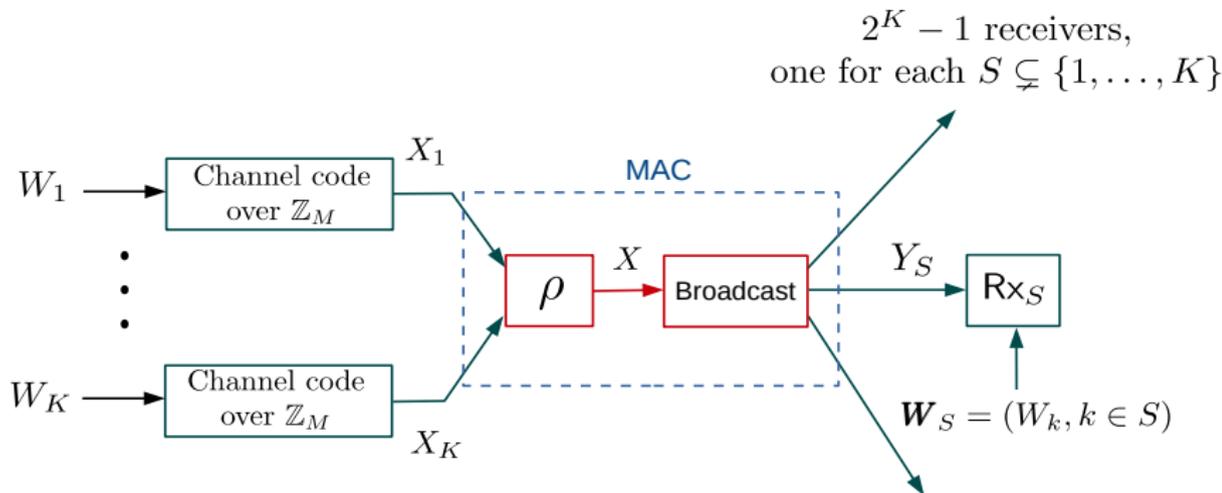
- The binary index code reduces the codeword length N (hence, the constellation size) while meeting the demands of the receivers
- The bit labelling of QAM/PSK allows receivers with sufficient side information to achieve gains in minimum Euclidean distance

Coded Index Modulation



- concatenated scheme: coding gain + side information gain.
- converts the channel into a MAC with many receivers.
- can perform close to channel capacity.

Coded Index Modulation



- If minimum Hamming distance of channel codes is d_H , then minimum squared Euclidean distance at Rx_S is at least $d_H \times d_S^2$.
- Capacity of MAC with many receivers: Ulrey Inf. & Cont. '75

Achievable rate region

Notation:

- $2^K - 1$ receivers indexed by S .
- $\text{Rx}_S = (\text{SNR}_S, S)$ observes Y_S .
- $\mathbf{X}_S = (X_k, k \in S)$, $\mathbf{X}_{S^c} = (X_k, k \notin S)$.
- X_1, \dots, X_K have distributions $p(x_1), \dots, p(x_K)$.
- Inner code/modulation (ρ, \mathcal{X}) has dimension n .

Assumption:

- If $S \subset S'$, then $\text{SNR}_S \geq \text{SNR}_{S'}$

Theorem

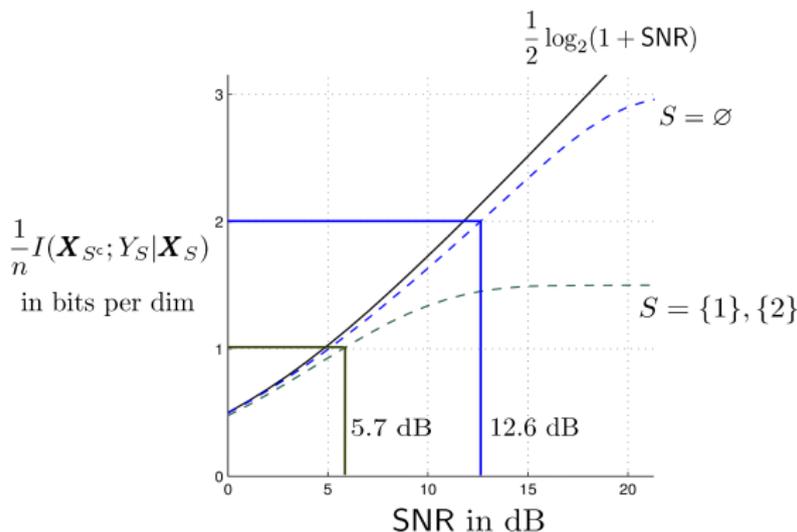
(R_1, \dots, R_K) achievable if and only if for every Rx_S :

$$\frac{1}{n} I(\mathbf{X}_{S^c}; Y_S | \mathbf{X}_S) \geq R - R_S.$$

$K = 2$, 64-QAM, $\Gamma = 4.66$ dB/b/dim

- Want $R_1 = R_2 = 1$ b/dim
- $2^K - 1 = 3$ receivers: $S = \emptyset, \{1\}, \{2\}$

$$\frac{1}{n} I(\mathbf{X}_{S^c}; Y_S | \mathbf{X}_S) \geq \begin{cases} R_1 + R_2 = 2 & \text{if } S = \emptyset \\ R_2 = 1 & \text{if } S = \{1\} \\ R_1 = 1 & \text{if } S = \{2\} \end{cases}$$



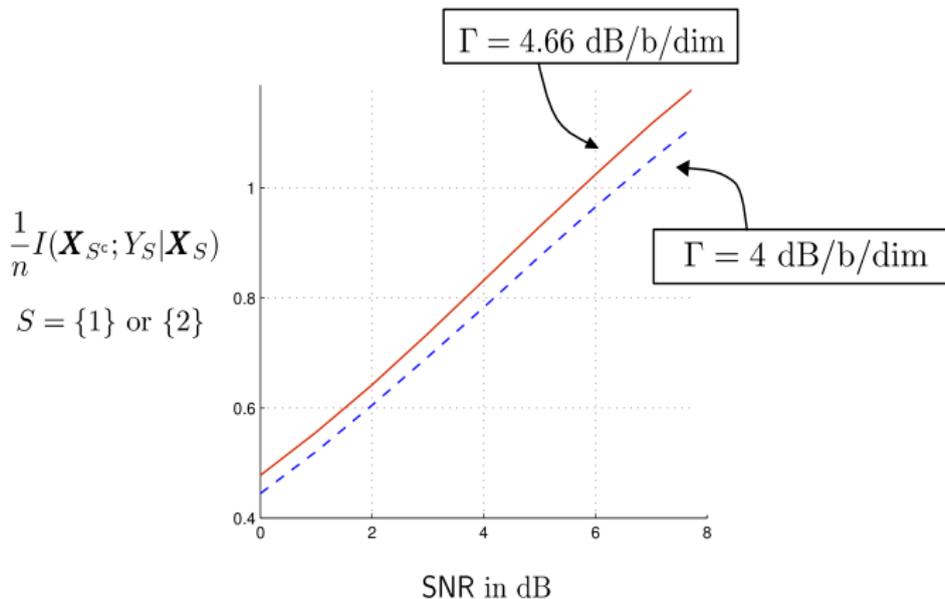
Dependence on Γ

- Larger $I(\mathbf{X}_{S^c}; Y_S | \mathbf{X}_S)$, for all $S \Rightarrow$ larger rates.
- Fano's inequality:

$$I(\mathbf{X}_{S^c}; Y_S | \mathbf{X}_S) \geq (1 - P_e(\mathbf{X}_{S^c} | Y_S, \mathbf{X}_S)) \log_2 \prod_{k \in S^c} |\mathcal{X}_k| - 1$$

- Larger $\Gamma \Rightarrow$ larger d_S for all $S \Rightarrow$ smaller P_e simultaneously for all S
- We expect a modulation with larger Γ to perform better.

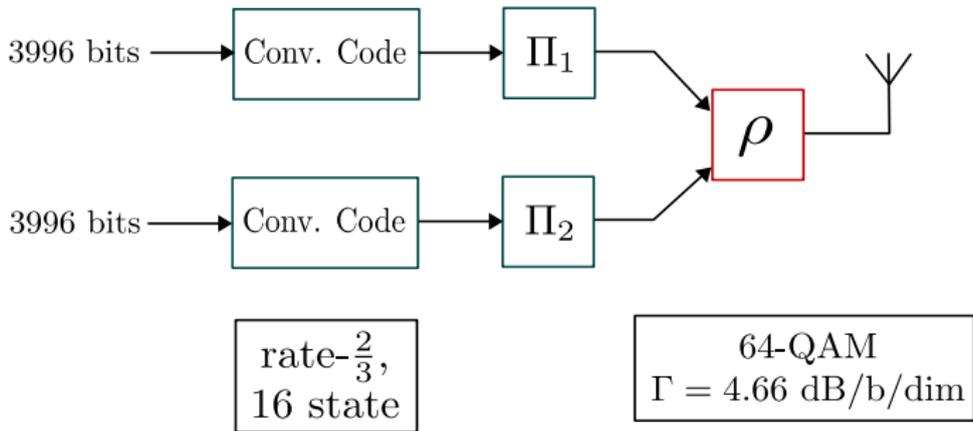
Example: 64-QAM, $K = 2$ messages



SNR gain of 0.7 dB at $\frac{1}{n} I(\mathbf{X}_{S^c}; Y_S | \mathbf{X}_S) = 1$.

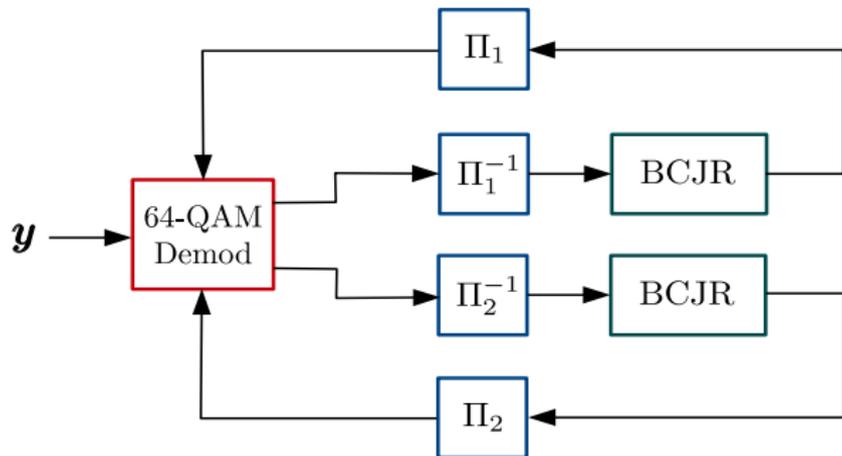
Encoder

- $K = 2$ messages, $R_1 = R_2 = 1$ b/dim.

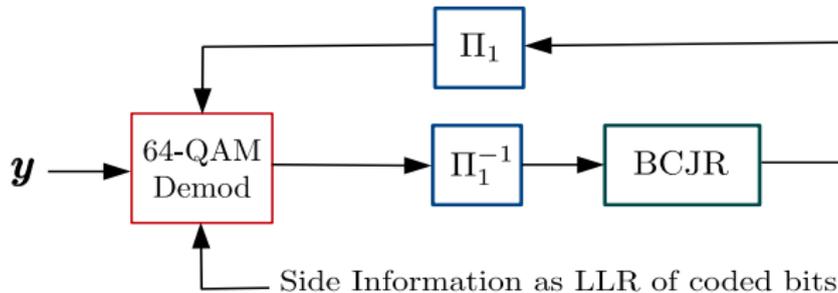


Decoder

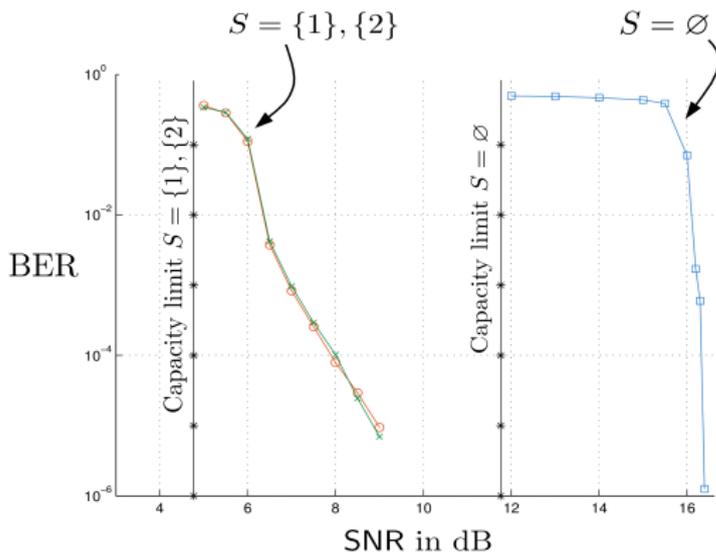
$$\underline{S = \emptyset}$$



$$\underline{S = \{2\}}$$



Simulation Result



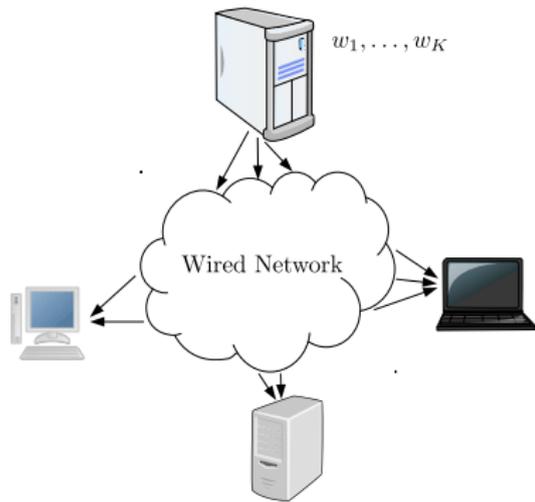
Gap to capacity (with Gaussian input alphabet) at BER 10^{-4} :

- 3.3 dB for $S = \{1\}, \{2\}$.
- 4.2 dB for $S = \emptyset$.

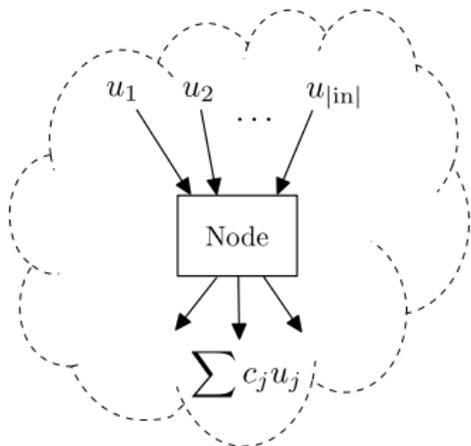
Wireline Multicasting

(Koetter & Médard T-IT Mar '03)

Multicast network



Linear network coding over \mathbb{F}_q

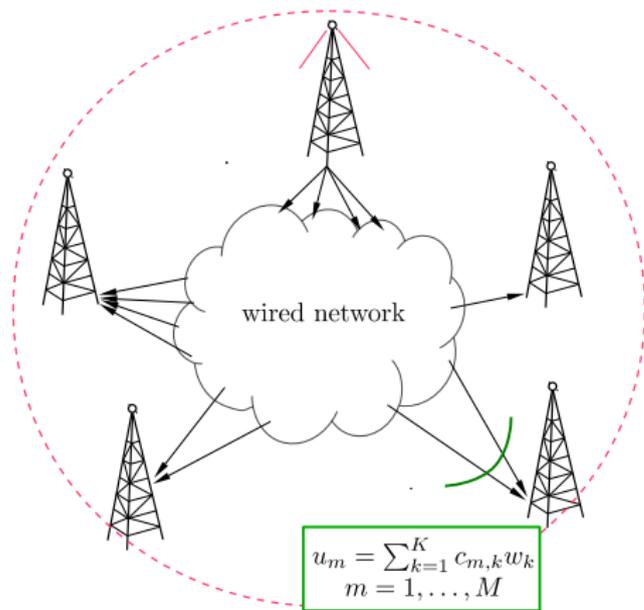


A network coding solution exists iff $\text{max-flow} \geq K$.

max-flow = maximum number of edge-disjoint paths from the source to each of the receivers

Broadcasting with Coded Side Information at the Receivers

(Natarajan, Hong, Viterbo arXiv:1509.01332)



- Suppose $\text{max-flow} < K$.
- A wireless signal can supplement the wireline network.
- Symbols from wireline network serve as side information to decode wireless signal: linear combinations of source messages
- \Rightarrow Broadcasting with coded side information at the receivers

Theorem: Lattice codes achieve the capacity of a wireless broadcast channel with coded side information at the receivers

References

Wireline Multicasting

- R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Trans. Netw.* vol. 11, no. 5, pp. 782–795, Oct. 2003.

Index Codes for the Gaussian broadcast channel

- L. Natarajan, Y. Hong, and E. Viterbo, “Lattice index coding,” *IEEE Trans. Inf. Theory*, pp. 6505–6525, Dec. 2015.
- —, “Lattice Index Coding for the Broadcast Channel,” in *Proc. IEEE Inf. Theory Workshop (ITW)*, Apr. 2015.
- Y.-C. Huang, “Lattice index codes from algebraic number fields,” in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2015, pp. 2485–2489.
- L. Natarajan, Y. Hong, and E. Viterbo, “Index codes for the Gaussian broadcast channel using quadrature amplitude modulation,” *IEEE Commun. Lett.*, pp. 1291–1294, Aug. 2015.
- A. A. Mahesh and B. S. Rajan, “Noisy index coding with PSK and QAM,” arXiv:1603.03152, Mar. 2016.
- L. Natarajan, Y. Hong, and E. Viterbo, “Capacity of coded index modulation,” in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2015, pp. 596–600.
- —, “Lattice codes achieve the capacity of Gaussian broadcast channels with coded side information,” Submitted to *IEEE Trans. Inf. Theory*, arxiv:1509.01332, Sep. 2015.