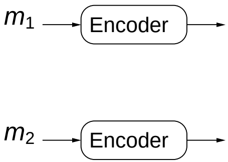
The Degrees of Freedom of Compute-and-Forward

Urs Niesen
Jointly with Phil Whiting

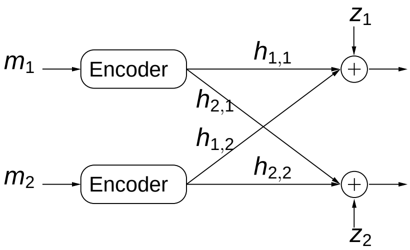
Bell Labs, Alcatel-Lucent

Problem Setting



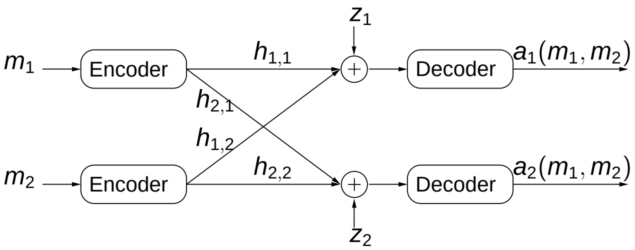
- K transmitters, messages $m_1, \ldots, m_K$, power constraint P

Problem Setting



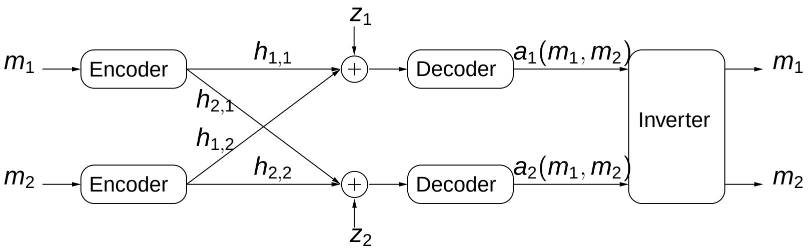
- K transmitters, messages $m_1, \ldots, m_K$, power constraint P
- Gaussian channel with constant gains $\boldsymbol{H} = \{h_{\ell,k}\}$

Problem Setting



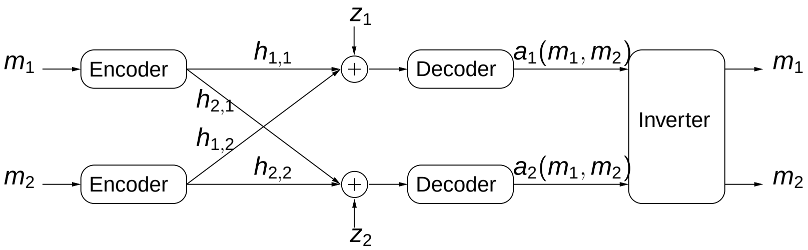
- K transmitters, messages $m_1, \ldots, m_K$, power constraint P
- Gaussian channel with constant gains $\boldsymbol{H} = \{h_{\ell,k}\}$
- Decode any deterministic function a_ℓ of the messages $m_1, \ldots, m_K$

Problem Setting



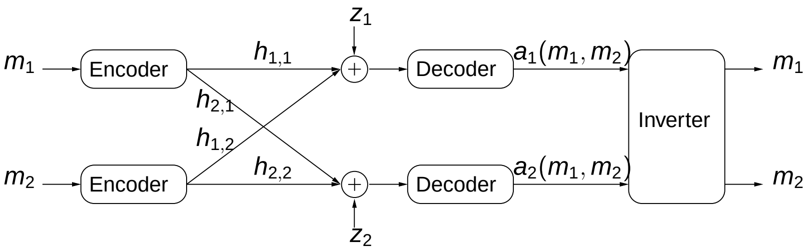
- K transmitters, messages $m_1, \ldots, m_K$, power constraint P
- Gaussian channel with constant gains $\boldsymbol{H} = \{h_{\ell,k}\}$
- Decode any deterministic function a_ℓ of the messages $m_1, \ldots, m_K$
- Invert all computed functions $a_1, \ldots, a_K$ to recover the messages $m_1, \ldots, m_K$

Problem Setting



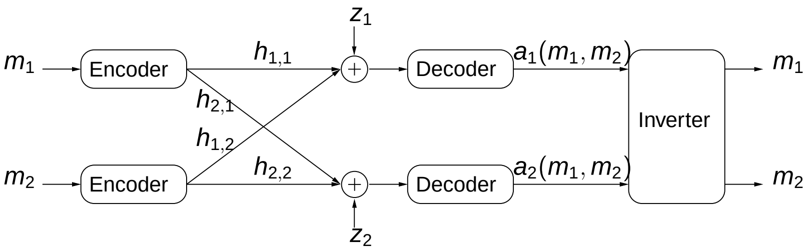
- Computation capacity $C(P, \boldsymbol{H}, \{a_\ell\})$ for fixed function $\{a_\ell\}$

Problem Setting



- Computation capacity $C(P, \boldsymbol{H}, \{a_\ell\})$ for fixed function $\{a_\ell\}$
- $C(P, \boldsymbol{H}, \boldsymbol{A})$ for linear function $\{a_\ell\}$

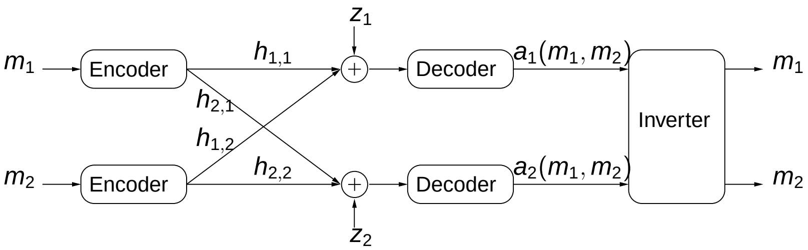
Problem Setting



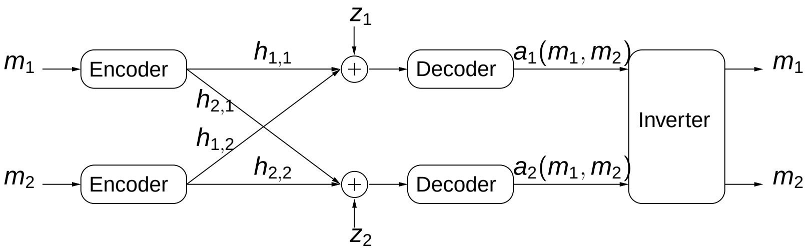
- Computation capacity $C(P, \boldsymbol{H}, \{a_\ell\})$ for fixed function $\{a_\ell\}$
- $C(P, \boldsymbol{H}, \boldsymbol{A})$ for linear function $\{a_\ell\}$
- Computation capacity

$$C(P, \boldsymbol{H}) \triangleq \max_{\{a_\ell\}} C(P, \boldsymbol{H}, \{a_\ell\})$$

with maximization over all invertible functions $\{a_\ell\}$



- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel

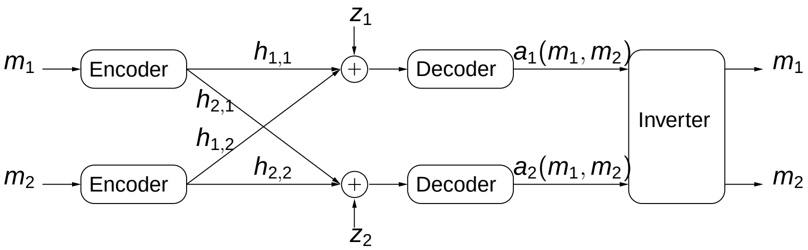


- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel

$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I})$$

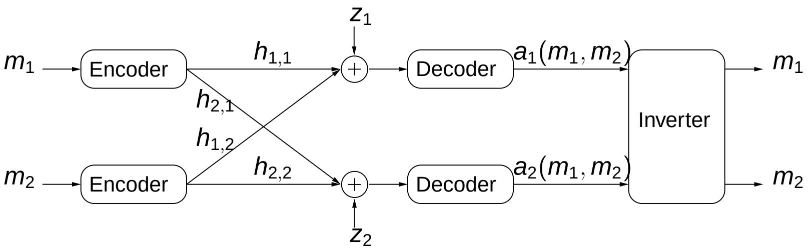
Computation Capacity

Some Special Cases and Bounds



- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel (Motahari et al. 2009)

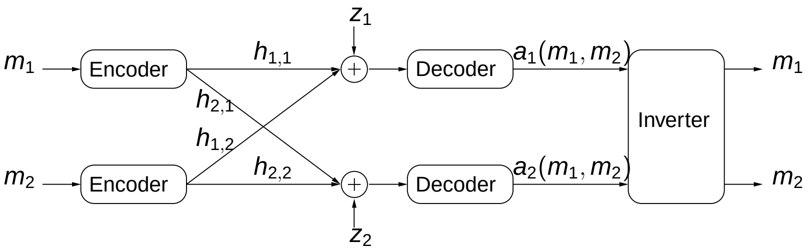
$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I}) = \frac{K}{4} \log(P) + o(\log(P))$$



- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel (Motahari et al. 2009)

$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I}) \Rightarrow \lim_{P \to \infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2} \log(P)} \geq K/2$$

Computation Capacity
Some Special Cases and Bounds



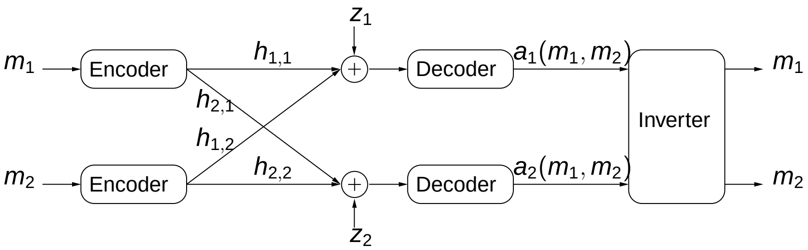
- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel (Motahari et al. 2009)

$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I}) \Rightarrow \lim_{P \to \infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} \geq K/2$$

- Allow cooperation among transmitters and among receivers $\Rightarrow K \times K$ MIMO channel

Computation Capacity

Some Special Cases and Bounds



- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel (Motahari et al. 2009)

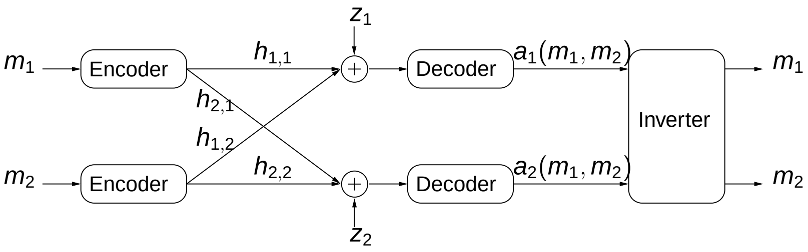
$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I}) \Rightarrow \lim_{P \to \infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2} \log(P)} \geq K/2$$

- Allow cooperation among transmitters and among receivers $\Rightarrow K \times K$ MIMO channel (Telatar 1999)

$$C(P, \boldsymbol{H}) \leq \max_{\boldsymbol{Q}} \frac{1}{2} \log \det(\boldsymbol{I} + \boldsymbol{HQH}^T)$$

Computation Capacity

Some Special Cases and Bounds

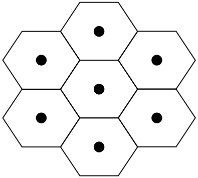


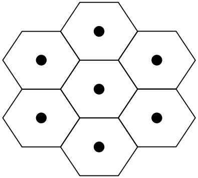
- Identity function $\boldsymbol{A} = \boldsymbol{I} \Rightarrow C(P, \boldsymbol{H}, \boldsymbol{I})$ is the capacity of the K-user interference channel (Motahari et al. 2009)

$$C(P, \boldsymbol{H}) \geq C(P, \boldsymbol{H}, \boldsymbol{I}) \Rightarrow \lim_{P \to \infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} \geq K/2$$

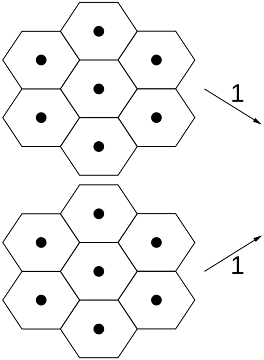
- Allow cooperation among transmitters and among receivers $\Rightarrow K \times K$ MIMO channel (Telatar 1999)

$$C(P, \boldsymbol{H}) \leq \max_{\boldsymbol{Q}} \tfrac{1}{2} \log\det(\boldsymbol{I} + \boldsymbol{HQH}^T) \Rightarrow \lim_{P \to \infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} \leq K$$

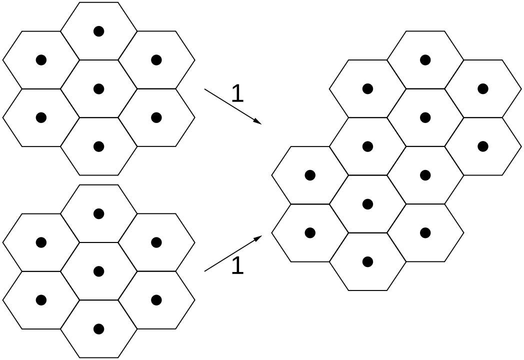




- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$



- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$

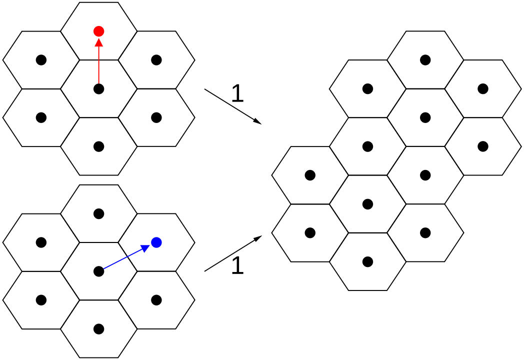


- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$

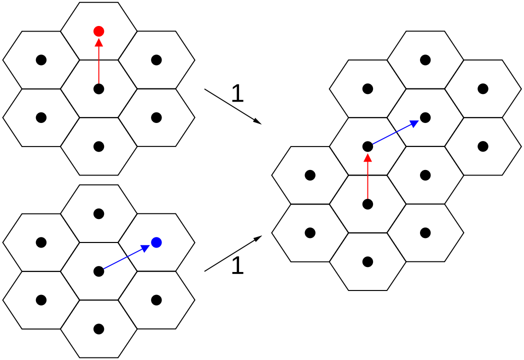
Computation Capacity

Lattice Codes

Nazer and Gastpar (2009)



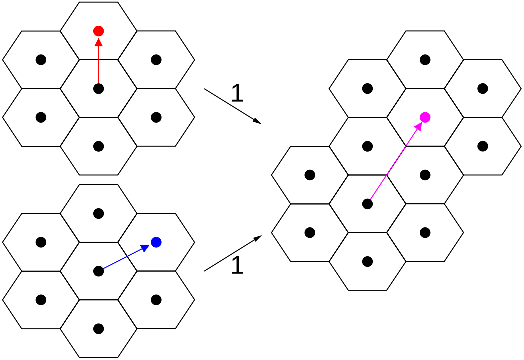
- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$



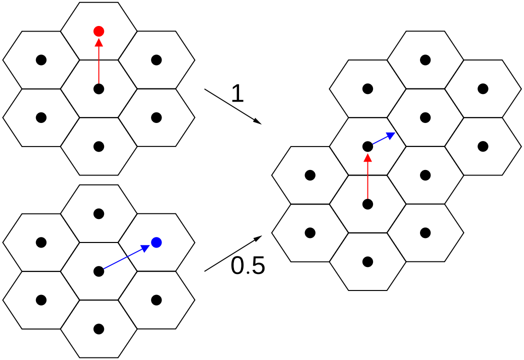
- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$

Computation Capacity
Lattice Codes

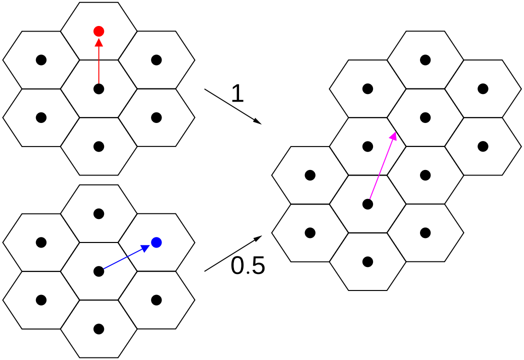
Nazer and Gastpar (2009)



- Two transmitters, one receiver, $\boldsymbol{h} = (1, 1)$
- Decode $\boldsymbol{a} = (1, 1)$



- Two transmitters, one receiver, $\boldsymbol{h} = (1, 0.5)$

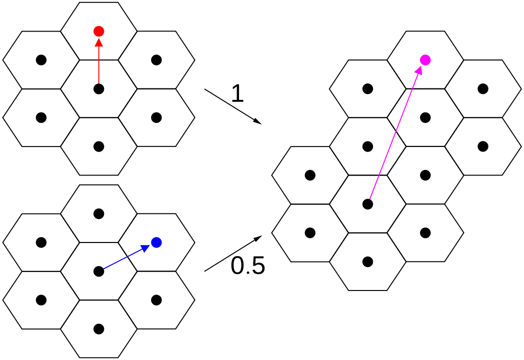


- Two transmitters, one receiver, $\boldsymbol{h} = (1, 0.5)$

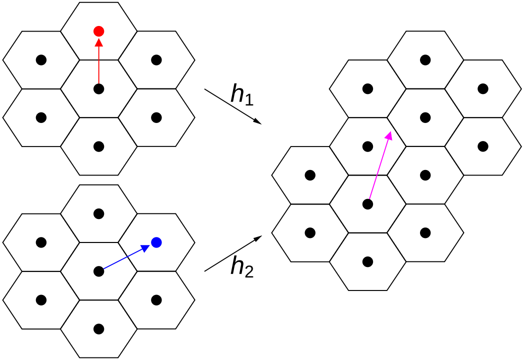
Computation Capacity

Lattice Codes

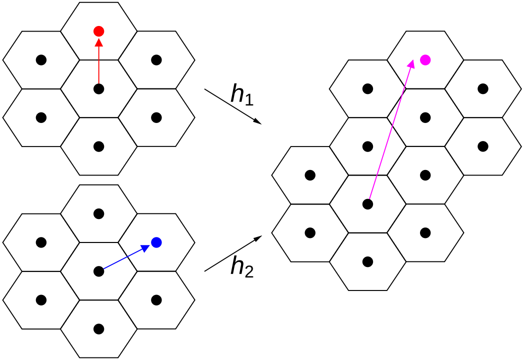
Nazer and Gastpar (2009)



- Two transmitters, one receiver, $\boldsymbol{h} = (1, 0.5)$
- Scale output by $\beta = 2$, decode $\boldsymbol{a} = (2, 1)$



- K transmitters, one receiver, $\boldsymbol{h} \in \mathbb{R}^K$

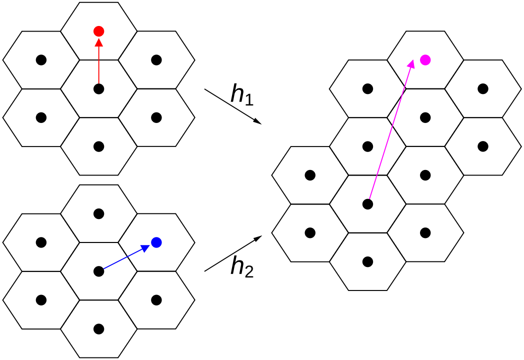


- K transmitters, one receiver, $\boldsymbol{h} \in \mathbb{R}^K$
- Scale output by $\beta \in \mathbb{R}$, decode $\boldsymbol{a} \in \mathbb{Z}^K$

Computation Capacity

Lattice Codes

Nazer and Gastpar (2009)

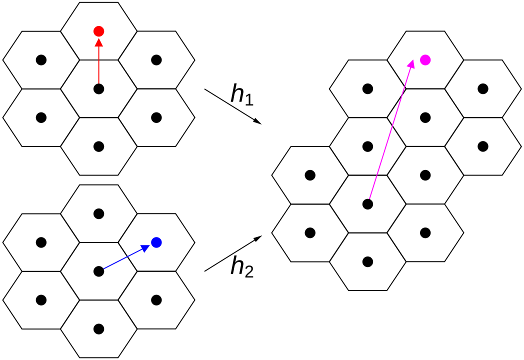


- K transmitters, one receiver, $\boldsymbol{h} \in \mathbb{R}^K$
- Scale output by $\beta \in \mathbb{R}$, decode $\boldsymbol{a} \in \mathbb{Z}^K$

$$C(P, \boldsymbol{h}, \boldsymbol{a}) \geq \max_{\beta} \frac{1}{2} \log \left(\frac{P}{\beta^2 + P \|\beta \boldsymbol{h} - \boldsymbol{a}\|^2} \right)$$

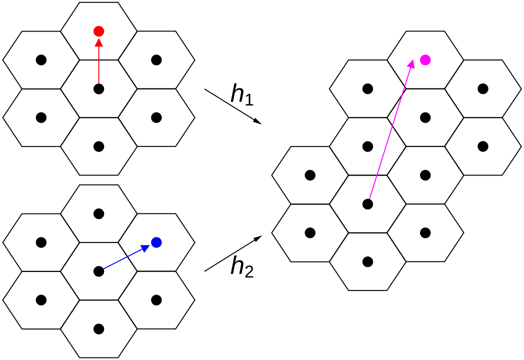
Computation Capacity
Lattice Codes

Nazer and Gastpar (2009)



- K transmitters, one receiver, $\boldsymbol{h} \in \mathbb{R}^K$
- Scale output by $\beta \in \mathbb{R}$, decode $\boldsymbol{a} \in \mathbb{Z}^K$

$$C(P, \boldsymbol{h}, \boldsymbol{a}) \geq \frac{1}{2} \log \left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$



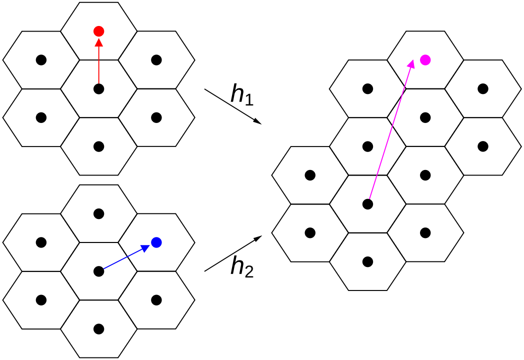
- K transmitters, one receiver, $\boldsymbol{h} \in \mathbb{R}^K$
- Scale output by $\beta \in \mathbb{R}$, decode $\boldsymbol{a} \in \mathbb{Z}^K$

$$C(P, \boldsymbol{h}, \boldsymbol{a}) \geq \frac{1}{2} \log \left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right) \triangleq R_L(P, \boldsymbol{h}, \boldsymbol{a})$$

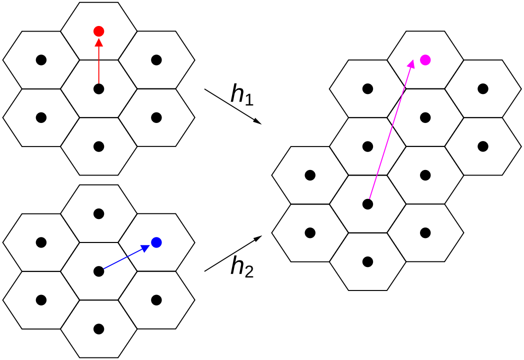
Computation Capacity

Lattice Codes

Nazer and Gastpar (2009)

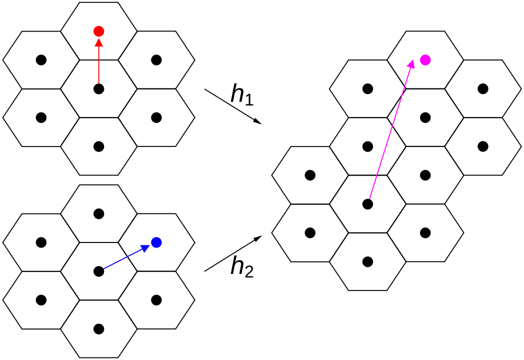


- K transmitters, K receivers, $\boldsymbol{H} \in \mathbb{R}^{K \times K}$
- Decode $\boldsymbol{A} \in \mathbb{Z}^{K \times K}$



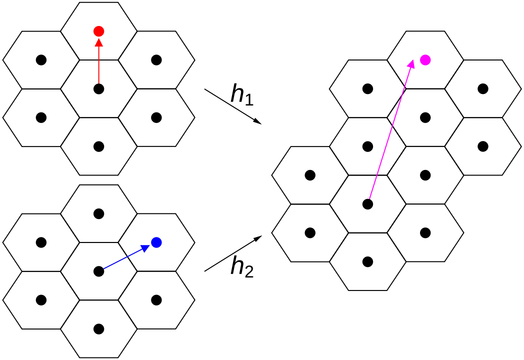
- K transmitters, K receivers, $\boldsymbol{H} \in \mathbb{R}^{K \times K}$
- Decode $\boldsymbol{A} \in \mathbb{Z}^{K \times K}$

$$C(P, \boldsymbol{H}, \boldsymbol{A}) \geq \qquad R_L(P, \boldsymbol{H}, \boldsymbol{A})$$



- K transmitters, K receivers, $\boldsymbol{H} \in \mathbb{R}^{K \times K}$
- Decode $\boldsymbol{A} \in \mathbb{Z}^{K \times K}$

$$\max_{\boldsymbol{A}} C(P, \boldsymbol{H}, \boldsymbol{A}) \geq \max_{\boldsymbol{A}} R_L(P, \boldsymbol{H}, \boldsymbol{A})$$



- K transmitters, K receivers, $\boldsymbol{H} \in \mathbb{R}^{K \times K}$
- Decode $\boldsymbol{A} \in \mathbb{Z}^{K \times K}$

$$C(P, \boldsymbol{H}) \geq R_L(P, \boldsymbol{H})$$

Questions

- We already know that the computation capacity satisfies

$$K/2 \leq \lim_{P\to\infty} \frac{C(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} \leq K$$

Questions

- We already know that the computation capacity satisfies

$$K/2 \leq \lim_{P\to\infty} \frac{C(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} \leq K$$

- What are the degrees of freedom of compute-and-forward

$$\lim_{P\to\infty} \frac{C(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = ?$$

Questions

- We already know that the computation capacity satisfies

$$K/2 \leq \lim_{P\to\infty} \frac{C(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} \leq K$$

- What are the degrees of freedom of compute-and-forward

$$\lim_{P\to\infty} \frac{C(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = ?$$

- What are the degrees of freedom achieved by lattice codes

$$\lim_{P\to\infty} \frac{R_L(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = ?$$

Performance of Lattice Codes

$$R_L(P, \boldsymbol{h}, \boldsymbol{a}) \triangleq \frac{1}{2} \log\left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$

Performance of Lattice Codes

$$R_L(P, \boldsymbol{h}, \boldsymbol{a}) \triangleq \frac{1}{2} \log \left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K \times K}$

Performance of Lattice Codes

$$R_L(P, \boldsymbol{h}, \boldsymbol{a}) \triangleq \frac{1}{2} \log \left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K \times K} \Rightarrow$ Set $\boldsymbol{A} = \boldsymbol{H} \in \mathbb{Z}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

Performance of Lattice Codes

$$R_L(P, \boldsymbol{h}, \boldsymbol{a}) \triangleq \frac{1}{2} \log\left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K \times K} \Rightarrow$ Set $\boldsymbol{A} = \boldsymbol{H} \in \mathbb{Z}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Rational channel gains $\boldsymbol{H} \in \mathbb{Q}^{K \times K}$

Performance of Lattice Codes

$$R_L(P, \boldsymbol{h}, \boldsymbol{a}) \triangleq \frac{1}{2} \log \left(\frac{1 + P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2 + P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2 - (\boldsymbol{h}^T\boldsymbol{a})^2\right)} \right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K \times K} \Rightarrow$ Set $\boldsymbol{A} = \boldsymbol{H} \in \mathbb{Z}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Rational channel gains $\boldsymbol{H} \in \mathbb{Q}^{K \times K} \Rightarrow$ Set $\boldsymbol{A} = q\boldsymbol{H} \in \mathbb{Z}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(P, \boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

Performance of Lattice Codes

$$R_L(P,\boldsymbol{h},\boldsymbol{a}) \triangleq \frac{1}{2}\log\left(\frac{1+P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2+P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2-(\boldsymbol{h}^T\boldsymbol{a})^2\right)}\right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K\times K} \Rightarrow$ Set $\boldsymbol{A} = \boldsymbol{H} \in \mathbb{Z}^{K\times K}$

$$\lim_{P\to\infty} \frac{R_L(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Rational channel gains $\boldsymbol{H} \in \mathbb{Q}^{K\times K} \Rightarrow$ Set $\boldsymbol{A} = q\boldsymbol{H} \in \mathbb{Z}^{K\times K}$

$$\lim_{P\to\infty} \frac{R_L(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Real channel gains $\boldsymbol{H} \in \mathbb{R}^{K\times K}$

Performance of Lattice Codes

$$R_L(P,\boldsymbol{h},\boldsymbol{a}) \triangleq \frac{1}{2}\log\left(\frac{1+P\|\boldsymbol{h}\|^2}{\|\boldsymbol{a}\|^2+P\left(\|\boldsymbol{a}\|^2\|\boldsymbol{h}\|^2-(\boldsymbol{h}^T\boldsymbol{a})^2\right)}\right)$$

- Integer channel gains $\boldsymbol{H} \in \mathbb{Z}^{K\times K} \Rightarrow$ Set $\boldsymbol{A} = \boldsymbol{H} \in \mathbb{Z}^{K\times K}$

$$\lim_{P\to\infty} \frac{R_L(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Rational channel gains $\boldsymbol{H} \in \mathbb{Q}^{K\times K} \Rightarrow$ Set $\boldsymbol{A} = q\boldsymbol{H} \in \mathbb{Z}^{K\times K}$

$$\lim_{P\to\infty} \frac{R_L(P,\boldsymbol{H})}{\frac{1}{2}\log(P)} = K$$

- Real channel gains $\boldsymbol{H} \in \mathbb{R}^{K\times K} \Rightarrow$?

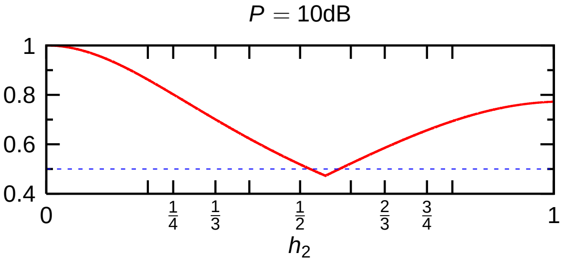
Performance of Lattice Codes

- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$

Performance of Lattice Codes

- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$

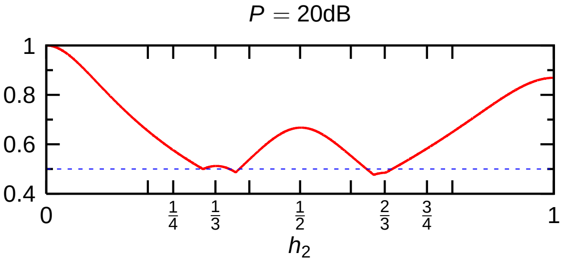
Performance of Lattice Codes



- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\boldsymbol{0}\}$

$$\frac{\max_{\boldsymbol{a}} R_L(P, \boldsymbol{h}, \boldsymbol{a})}{\frac{1}{2}\log(1 + \|\boldsymbol{h}\|^2 P)}$$

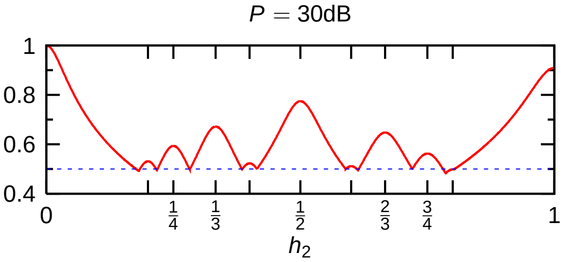
Performance of Lattice Codes



- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$

$$\frac{\max_{\boldsymbol{a}} R_L(P, \boldsymbol{h}, \boldsymbol{a})}{\frac{1}{2}\log(1 + \|\boldsymbol{h}\|^2 P)}$$

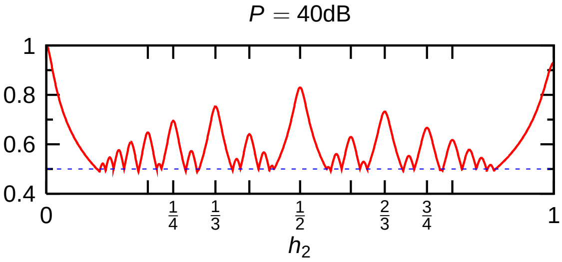
Performance of Lattice Codes



- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$

$$\frac{\max_{\boldsymbol{a}} R_L(P, \boldsymbol{h}, \boldsymbol{a})}{\frac{1}{2}\log(1 + \|\boldsymbol{h}\|^2 P)}$$

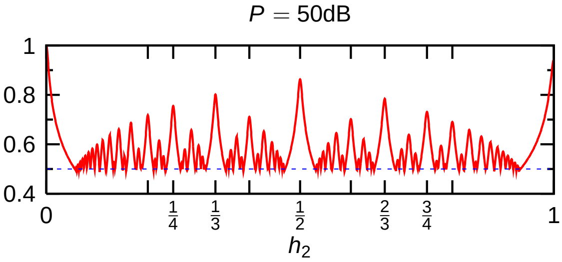
Performance of Lattice Codes



- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$

$$\frac{\max_{\boldsymbol{a}} R_L(P, \boldsymbol{h}, \boldsymbol{a})}{\frac{1}{2}\log(1 + \|\boldsymbol{h}\|^2 P)}$$

Performance of Lattice Codes



- Two transmitters, one receiver, $\boldsymbol{h} = (1, h_2)$
- Optimize over coefficients $\boldsymbol{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$

$$\frac{\max_{\boldsymbol{a}} R_L(P, \boldsymbol{h}, \boldsymbol{a})}{\frac{1}{2}\log(1 + \|\boldsymbol{h}\|^2 P)}$$

Performance of Lattice Codes

Theorem 1

For any $K \geq 2$ and almost every $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} \leq \frac{2}{1 + 1/K} \leq 2.$$

Performance of Lattice Codes

Theorem 1

For any $K \geq 2$ *and almost every* $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} \leq \frac{2}{1 + 1/K} \leq 2.$$

Compare to:

- MIMO upper bound of K on the degrees of freedom of compute-and-forward

Performance of Lattice Codes

Theorem 1

For any $K \geq 2$ *and almost every* $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{R_L(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} \leq \frac{2}{1 + 1/K} \leq 2.$$

Compare to:

- MIMO upper bound of K on the degrees of freedom of compute-and-forward
- Decode-and-forward lower bound of $K/2$ on the degrees of freedom compute-and-forward

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR?

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR? $\Rightarrow$ Yes!

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR? $\Rightarrow$ Yes!

Theorem 2

For any $K \geq 2$ and almost every $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{C(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} = K\,.$$

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR? $\Rightarrow$ Yes!

Theorem 2

For any $K \geq 2$ and almost every $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{C(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} = K.$$

- Compute-and-forward achieves MIMO upper bound of K degrees of freedom
- Invertible functions can be encoded/decoded distributedly at same asymptotic rate as the centralized scheme

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR? $\Rightarrow$ Yes!

Theorem 2

For any $K \geq 2$ and almost every $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$\lim_{P \to \infty} \frac{C(\boldsymbol{H}, P)}{\frac{1}{2}\log(P)} = K .$$

- Compute-and-forward achieves MIMO upper bound of K degrees of freedom
- Invertible functions can be encoded/decoded distributedly at same asymptotic rate as the centralized scheme
- Compute-and-forward achieves twice the degrees of freedom of decode-and-forward

Degrees of Freedom of Compute-and-Forward

Is compute-and-forward useful at high SNR? $\Rightarrow$ Yes!

Theorem 2

For any $K \geq 2$ and almost every $\boldsymbol{H} \in \mathbb{R}^{K \times K}$

$$-O\left(\log^{K^2/(1+K^2)}(P)\right) \leq C(\boldsymbol{H}, P) - \frac{1}{2}K \log(P) \leq O(1).$$

- Compute-and-forward achieves MIMO upper bound of K degrees of freedom
- Invertible functions can be encoded/decoded distributedly at same asymptotic rate as the centralized scheme
- Compute-and-forward achieves twice the degrees of freedom of decode-and-forward

Lower Bound in Theorem 2

- Channel computes noisy linear combinations with real coefficients

Lower Bound in Theorem 2

- Channel computes noisy linear combinations with real coefficients
- Lattice codes transform this into a system computing noiseless linear combinations with integer coefficients

Lower Bound in Theorem 2

- Channel computes noisy linear combinations with real coefficients
- Lattice codes transform this into a system computing noiseless linear combinations with integer coefficients
- The achievable scheme in Theorem 2 opts instead to implement these two functions separately

Lower Bound in Theorem 2

- Channel computes noisy linear combinations with real coefficients
- Lattice codes transform this into a system computing noiseless linear combinations with integer coefficients
- The achievable scheme in Theorem 2 opts instead to implement these two functions separately
- Use signal alignment to transform real linear combinations into integer linear combinations

Lower Bound in Theorem 2

- Channel computes noisy linear combinations with real coefficients
- Lattice codes transform this into a system computing noiseless linear combinations with integer coefficients
- The achievable scheme in Theorem 2 opts instead to implement these two functions separately
- Use signal alignment to transform real linear combinations into integer linear combinations
- Use a linear outer code to transform noisy linear combinations into noiseless linear combinations

Lower Bound in Theorem 2
Outline

- Channel computes noisy linear combinations with real coefficients

$$h_{1,1}m_1 + h_{1,2}m_2 + z_1$$

Lower Bound in Theorem 2

Outline

- Channel computes noisy linear combinations with real coefficients

$$h_{1,1}m_1 + h_{1,2}m_2 + z_1$$

- Use signal alignment to transform real linear combinations into integer linear combinations

$$a_{1,1}m_1 + a_{1,2}m_2 + z_1$$

Lower Bound in Theorem 2

Outline

- Channel computes noisy linear combinations with real coefficients

$$h_{1,1}m_1 + h_{1,2}m_2 + z_1$$

- Use signal alignment to transform real linear combinations into integer linear combinations

$$a_{1,1}m_1 + a_{1,2}m_2 + z_1$$

$\Rightarrow$ Split each message into several submessages
$\Rightarrow$ Use tools from Diophantine approximation

Lower Bound in Theorem 2

Outline

- Channel computes noisy linear combinations with real coefficients

$$h_{1,1}m_1 + h_{1,2}m_2 + z_1$$

- Use signal alignment to transform real linear combinations into integer linear combinations

$$a_{1,1}m_1 + a_{1,2}m_2 + z_1$$

$\Rightarrow$ Split each message into several submessages
$\Rightarrow$ Use tools from Diophantine approximation

- Use a linear outer code to transform noisy linear combinations into noiseless linear combinations

$$a_{1,1}m_1 + a_{1,2}m_2$$

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

Lower Bound in Theorem 2

Preliminaries

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

- Let $x_k = A q_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$

Lower Bound in Theorem 2

Preliminaries

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\big((\max_i |q_i|)^{1-K-\varepsilon} \big).$$

- Let $x_k = Aq_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

- Let $x_k = A q_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$
- Minimum distance between $(x_1, \ldots, x_K) \neq (x_1', \ldots, x_K')$

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

- Let $x_k = A q_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$
- Minimum distance between $(x_1, \ldots, x_K) \neq (x_1', \ldots, x_K')$

$$\left| \sum_{k=1}^{K} h_k (x_k - x_k') \right|$$

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

- Let $x_k = Aq_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$
- Minimum distance between $(x_1, \ldots, x_K) \neq (x'_1, \ldots, x'_K)$

$$\left| \sum_{k=1}^{K} h_k (x_k - x'_k) \right| = A \left| \sum_{k=1}^{K} h_k (q_k - q'_k) \right|$$

Lower Bound in Theorem 2

Preliminaries

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\big((\max_i |q_i|)^{1-K-\varepsilon}\big).$$

- Let $x_k = Aq_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$
- Minimum distance between $(x_1, \ldots, x_K) \neq (x'_1, \ldots, x'_K)$

$$\left| \sum_{k=1}^{K} h_k (x_k - x'_k) \right| = A \left| \sum_{k=1}^{K} h_k (q_k - q'_k) \right| \gtrsim A\Omega(Q^{1-K})$$

Lower Bound in Theorem 2

Preliminaries

Groshev's Theorem

For any $\varepsilon > 0$, and almost all $(h_1, h_2, \ldots, h_K) \in \mathbb{R}^K$,

$$\min_{q_i \in \mathbb{Z}} \left| h_1 q_1 + \ldots + h_K q_K \right| \geq \Omega\left((\max_i |q_i|)^{1-K-\varepsilon} \right).$$

- Let $x_k = A q_k$ with $q_k \in \{-Q, -Q+1, \ldots, Q-1, Q\}$
- Assume we observe $y = h_1 x_1 + \ldots + h_K x_K + z$
- Minimum distance between $(x_1, \ldots, x_K) \neq (x_1', \ldots, x_K')$

$$\left| \sum_{k=1}^K h_k (x_k - x_k') \right| = A \left| \sum_{k=1}^K h_k (q_k - q_k') \right| \gtrsim A \Omega(Q^{1-K})$$

- For $A \approx P^{(K-1)/2K}$ and $Q \approx P^{1/2K}$ satisfy power constraint and can remove noise

Lower Bound in Theorem 2
Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

Lower Bound in Theorem 2
Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11}$$
$$x_2/A = q_{21}$$

Lower Bound in Theorem 2
Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11}$$
$$x_2/A = q_{21}$$

- This is received as

$$y_1/A = (q_{11} + q_{21})$$
$$y_2/A = q_{11} + hq_{21}$$

Lower Bound in Theorem 2

Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11} + hq_{12}$$
$$x_2/A = q_{21} + hq_{22}$$

- This is received as

$$y_1/A = (q_{11} + q_{21})$$
$$y_2/A = q_{11} + hq_{21}$$

Lower Bound in Theorem 2

Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11} + hq_{12}$$
$$x_2/A = q_{21} + hq_{22}$$

- This is received as

$$y_1/A = (q_{11} + q_{21}) + h(q_{12} + q_{22})$$
$$y_2/A = q_{11} + h(q_{21} + q_{12}) + h^2 q_{22}$$

Lower Bound in Theorem 2

Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11} + hq_{12} + \dots$$
$$x_2/A = q_{21} + hq_{22} + \dots$$

- This is received as

$$y_1/A = (q_{11} + q_{21}) + h(q_{12} + q_{22}) + \dots$$
$$y_2/A = q_{11} + h(q_{21} + q_{12}) + h^2 q_{22} + \dots$$

Lower Bound in Theorem 2
Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11} + hq_{12} + \dots$$
$$x_2/A = q_{21} + hq_{22} + \dots$$

- This is received as

$$y_1/A = (q_{11} + q_{21}) + h(q_{12} + q_{22}) + \dots$$
$$y_2/A = q_{11} + h(q_{21} + q_{12}) + h^2 q_{22} + \dots$$

- Groshev's Theorem to separate equations

Lower Bound in Theorem 2

Signal Alignment

Consider a simple interference channel without noise

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + hx_2$$

- Set

$$x_1/A = q_{11} + hq_{12} + \dots$$
$$x_2/A = q_{21} + hq_{22} + \dots$$

- This is received as

$$y_1/A = (q_{11} + q_{21}) + h(q_{12} + q_{22}) + \dots$$
$$y_2/A = q_{11} + h(q_{21} + q_{12}) + h^2 q_{22} + \dots$$

- Groshev's Theorem to separate equations
- Linear outer code to drive probability of error to zero

Summary

- Compute-and-forward as communication strategy for wireless networks

Summary

- Compute-and-forward as communication strategy for wireless networks
- Lattice codes achieve at most 2 degrees of freedom over a $K \times K$ channel

Summary

- Compute-and-forward as communication strategy for wireless networks
- Lattice codes achieve at most 2 degrees of freedom over a $K \times K$ channel
- However, a different implementation of compute-and-forward achieves K degrees of freedom

Summary

- Compute-and-forward as communication strategy for wireless networks
- Lattice codes achieve at most 2 degrees of freedom over a $K \times K$ channel
- However, a different implementation of compute-and-forward achieves K degrees of freedom
- Matches MIMO upper bound of K degrees of freedom

Summary

- Compute-and-forward as communication strategy for wireless networks
- Lattice codes achieve at most 2 degrees of freedom over a $K \times K$ channel
- However, a different implementation of compute-and-forward achieves K degrees of freedom
- Matches MIMO upper bound of K degrees of freedom
- Compute-and-forward achieves twice the degrees of freedom of decode-and-forward