Distributed Storage Codes Meet Multiple-Access Wiretap Channels

Dimitris Papailiopoulos and Alex Dimakis

USC

Allerton 2010

Overview

- MDS Storage Codes
- Minimize Repair Bandwidth
- Interference Alignment
- $\mathcal{R}$: Rank Constrained sumRank Minimization (over field)

- Multiple-Access Compound Wiretap Channel
- Maximize S-DoF
- Interference Alignment
- $\mathcal{V}$: Rank Constrained maxRank Minimization

We establish a connection.

Overview

- MDS Storage Codes
- Minimize Repair Bandwidth
- Interference Alignment
- $\mathcal{R}$: Rank Constrained sumRank Minimization (over field)

- Multiple-Access Compound Wiretap Channel
- Maximize S-DoF
- Interference Alignment
- $\mathcal{V}$: Rank Constrained maxRank Minimization

We establish a connection.

Overview

- MDS Storage Codes
- Minimize Repair Bandwidth
- Interference Alignment
- $\mathcal{R}$: Rank Constrained sumRank Minimization (over field)

- Multiple-Access Compound Wiretap Channel
- Maximize S-DoF
- Interference Alignment
- $\mathcal{V}$: Rank Constrained maxRank Minimization

We establish a connection.

Connection

- For *good* storage MDS codes and *good* multiple-access wiretap channels.

$$\boxed{\text{min(repair BW)} \equiv \text{max(S-DoF)}}$$

i.e. if I can solve one, I can solve the other.

- Good storage codes $\leftrightarrow$ Good multiple-access wiretap channels
- Good repair strategies $\leftrightarrow$ Good beamforming strategies

(over the same field)

Connection

- For *good* storage MDS codes and *good* multiple-access wiretap channels.

$$\boxed{\text{min(repair BW)} \equiv \text{max(S-DoF)}}$$

i.e. if I can solve one, I can solve the other.

- Good storage codes $\leftrightarrow$ Good multiple-access wiretap channels
- Good repair strategies $\leftrightarrow$ Good beamforming strategies

(over the same field)

Byproduct: We characterize the S-DoF of the SISO multiple-access compound wiretap channel.

How? By using as beamforming matrices, the repair matrices of a diagonal code by [CJM10], [SR10].

[Khisti], [Bagherikaram, Motahari,Khandani],
[Koyluoglu, El Gamal, Lai, Poor], [Kobayashi, Piantanida, Yang, Shamai], [He, Yener], [Bassily, Ulukus]

- Minimizing the Repair BW
- Maximizing the S-DoF
- Establishing the Connection
- The S-DoF of SISO Multiple-Access Compound Wiretap Channel
- Extensions and Conclusions

The Repair Problem

- Cut a file into 3 parts $\mathbf{a}, \mathbf{b}, \mathbf{c}$. Store it accross 5 nodes, rate $= \frac{3}{5}$. Each part has length $2N$.
- We use $(5, 3)$ MDS codes.
  1. Each node stores $2N$. 2. Any 3 nodes know everything.

$$\mathbf{a}$$

$$\mathbf{b}$$

$$\mathbf{c}$$

1 $\mathbf{A}_1^T\mathbf{a} + \mathbf{B}_1^T\mathbf{b} + \mathbf{C}_1^T\mathbf{c}$

2 $\mathbf{A}_2^T\mathbf{a} + \mathbf{B}_2^T\mathbf{b} + \mathbf{C}_2^T\mathbf{c}$

- $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$: $2N \times 2N$

[Dimakis, Wu, Suh, Ramchandran], [Rashmi, Shah, Kumar]

The Repair Problem

- Cut a file into 3 parts $\mathbf{a}, \mathbf{b}, \mathbf{c}$. Store it accross 5 nodes, rate $= \frac{3}{5}$. Each part has length $2N$.
- We use $(5, 3)$ MDS codes.
  1. Each node stores $2N$. 2. Any 3 nodes know everything.

$$\boxed{\mathbf{a}}$$
$$\boxed{\mathbf{b}}$$
$$\boxed{\mathbf{c}}$$

$$1 \quad \boxed{\mathbf{A}_1^T\mathbf{a} + \mathbf{B}_1^T\mathbf{b} + \mathbf{C}_1^T\mathbf{c}}$$
$$2 \quad \boxed{\mathbf{A}_2^T\mathbf{a} + \mathbf{B}_2^T\mathbf{b} + \mathbf{C}_2^T\mathbf{c}}$$

- $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$: $2N \times 2N$

[Dimakis, Wu, Suh, Ramchandran], [Rashmi, Shah, Kumar]

The Repair Problem

- Q: If a disk fails? A: Exactly repair what was lost!

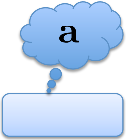
$\mathbf{a}$

$\mathbf{b}$

$\mathbf{c}$

1 $\mathbf{A}_1^T\mathbf{a} + \mathbf{B}_1^T\mathbf{b} + \mathbf{C}_1^T\mathbf{c}$

2 $\mathbf{A}_2^T\mathbf{a} + \mathbf{B}_2^T\mathbf{b} + \mathbf{C}_2^T\mathbf{c}$



- # unknowns in **a**: $2N$
-
-

The Repair Problem

- Q: If a disk fails? A: Exactly repair what was lost!

$\mathbf{a}$

$\mathbf{b}$

$\mathbf{c}$

1 $\mathbf{A}_1^T\mathbf{a}+\mathbf{B}_1^T\mathbf{b}+\mathbf{C}_1^T\mathbf{c}$ $\mathbf{R}_1$

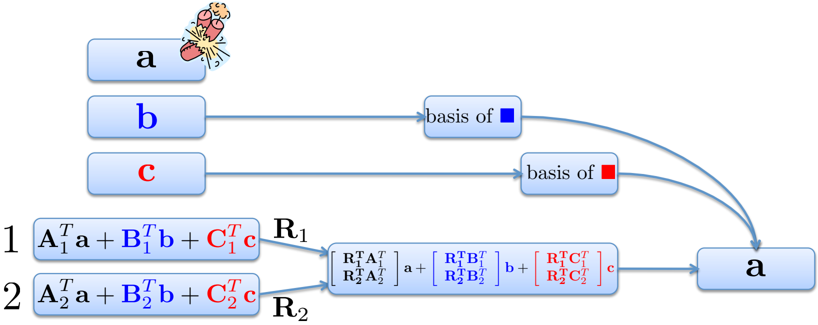
2 $\mathbf{A}_2^T\mathbf{a}+\mathbf{B}_2^T\mathbf{b}+\mathbf{C}_2^T\mathbf{c}$ $\mathbf{R}_2$

$$\begin{bmatrix}\mathbf{R}_1^T\mathbf{A}_1^T\\ \mathbf{R}_2^T\mathbf{A}_2^T\end{bmatrix}\mathbf{a}+\begin{bmatrix}\mathbf{R}_1^T\mathbf{B}_1^T\\ \mathbf{R}_2^T\mathbf{B}_2^T\end{bmatrix}\mathbf{b}+\begin{bmatrix}\mathbf{R}_1^T\mathbf{C}_1^T\\ \mathbf{R}_2^T\mathbf{C}_2^T\end{bmatrix}\mathbf{c}$$

- \# unknowns in $\mathbf{a}$: $2N$
- $\mathbf{R}_i$: $2N \times N$
- Q: Cost?

The Repair Problem

- Q: If a disk fails? A: Exactly repair what was lost!

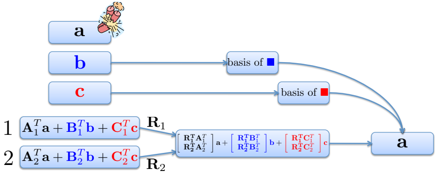


- $\#$ unknowns in $\mathbf{a}$: $2N$
- $\mathbf{R}_i : 2N \times N$
- Q: Cost? A: [Size of lost $\mathbf{a}$]+[$\#$ dimensions of ■ and ■].

The Repair Problem

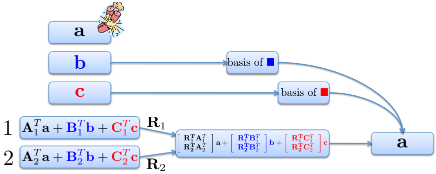
- Q1: How to find the minimum cost?
- A: Choose $\mathbf{R}_i$s so that interference spaces collapse to the smallest spaces possible $\Rightarrow$ **Interference Alignment**.
- Q2: Can you formalize this?
- A:

$$\mathcal{R}:\quad \min_{\mathbf{R}_1,\mathbf{R}_2} \left(\text{rank}\left(\blacksquare\right) + \text{rank}\left(\blacksquare\right)\right)$$
$$\text{s.t.}\quad \text{rank}\left(\blacksquare\right) = 2N$$



- Q1: How to find the minimum cost?
- A: Choose $\mathbf{R}_i$s so that interference spaces collapse to the smallest spaces possible $\Rightarrow$ **Interference Alignment**.
- Q2: Can you formalize this?
- A:

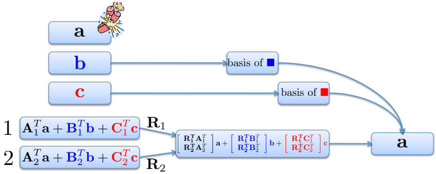
$$\boxed{\begin{aligned}&\mathcal{R}:\\ &\qquad \min_{\mathbf{R}_1,\mathbf{R}_2} \left(\text{rank}\left(\blacksquare\right) + \text{rank}\left(\blacksquare\right)\right)\\ &\text{s.t.}\ \ \text{rank}\left(\blacksquare\right) = 2N\end{aligned}}$$



- A special class of MDS codes: **Optimal** MDS codes. (a.k.a MSR codes)

$$\boxed{\text{Minimum Repair BW} = [\text{size of lost piece}] + 2 \times N}$$

- Any interference space can be squeezed into N dimensions.

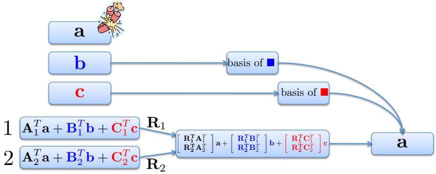


The Repair Problem

- A special class of MDS codes: **Optimal** MDS codes. (a.k.a MSR codes)

$$\boxed{\text{Minimum Repair BW} = [\text{size of lost piece}] + 2 \times N}$$

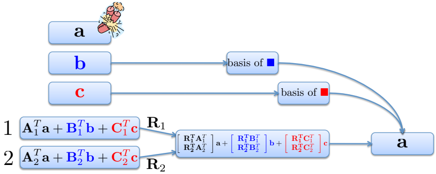
- Any interference space can be squeezed into N dimensions.



- A special class of MDS codes: **Optimal** MDS codes. (a.k.a MSR codes)

$$\boxed{\text{Minimum Repair BW} = [\text{size of lost piece}] + 2 \times N}$$

- Any interference space can be squeezed into N dimensions.

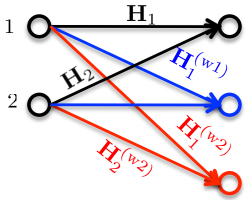


- Minimizing the Repair BW
- Maximizing the S-DoF
- Establishing the Connection
- The S-DoF of SISO Multiple-Access Compound Wiretap Channel
- Extensions and Conclusions

The S-DoF Problem

Multiple-access compound wiretap channel.

- System Model:
  2 users, each transmits N symbols,
  1 desired receiver, 2 wiretappers.



$$\mathbf{H}_1\mathbf{V}_1\mathbf{x}_1 + \mathbf{H}_2\mathbf{V}_2\mathbf{x}_2 + \mathbf{n} = [\mathbf{H}_1\mathbf{V}_1 \ \ \mathbf{H}_2\mathbf{V}_2] \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} + \mathbf{n}$$

$$\left[\mathbf{H}_1^{(w1)}\mathbf{V}_1 \ \ \mathbf{H}_2^{(w1)}\mathbf{V}_2\right]$$

$$\left[\mathbf{H}_1^{(w2)}\mathbf{V}_1 \ \ \mathbf{H}_2^{(w2)}\mathbf{V}_2\right]$$

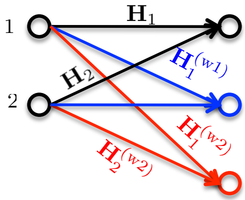
- $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2} : 2N \times 2N$,
- $\mathbf{V}_i : 2N \times N$
- Objective?
  S-DoF = [rank of ■]-max{[rank of ■], [rank of ■]}

  (outerbound $= 2N - N$)

The S-DoF Problem

Multiple-access compound wiretap channel.

- System Model:
  2 users, each transmits N symbols,
  1 desired receiver, 2 wiretappers.



$$\mathbf{H}_1\mathbf{V}_1\mathbf{x}_1 + \mathbf{H}_2\mathbf{V}_2\mathbf{x}_2 + \mathbf{n} = [\mathbf{H}_1\mathbf{V}_1 \;\; \mathbf{H}_2\mathbf{V}_2]\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} + \mathbf{n}$$

$$\left[\mathbf{H}_1^{(\mathrm{w1})}\mathbf{V}_1 \;\; \mathbf{H}_2^{(\mathrm{w1})}\mathbf{V}_2\right]$$

$$\left[\mathbf{H}_1^{(\mathrm{w2})}\mathbf{V}_1 \;\; \mathbf{H}_2^{(\mathrm{w2})}\mathbf{V}_2\right]$$

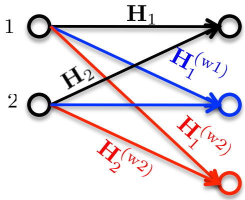
- $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2} : 2N \times 2N$,
- $\mathbf{V}_i : 2N \times N$
- Objective?
  S-DoF $=$ [rank of ■]-max{[rank of ■], [rank of ■]}

(outerbound $= 2N - N$)

The S-DoF Problem

Multiple-access compound wiretap channel.

- System Model:
  2 users, each transmits N symbols,
  1 desired receiver, 2 wiretappers.



$$\mathbf{H}_1\mathbf{V}_1\mathbf{x}_1 + \mathbf{H}_2\mathbf{V}_2\mathbf{x}_2 + \mathbf{n} = [\mathbf{H}_1\mathbf{V}_1 \ \ \mathbf{H}_2\mathbf{V}_2] \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} + \mathbf{n}$$

$$\left[\mathbf{H}_1^{(w1)}\mathbf{V}_1 \ \ \mathbf{H}_2^{(w1)}\mathbf{V}_2\right]$$

$$\left[\mathbf{H}_1^{(w2)}\mathbf{V}_1 \ \ \mathbf{H}_2^{(w2)}\mathbf{V}_2\right]$$

- $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2} : 2N \times 2N$,
- $\mathbf{V}_i : 2N \times N$
- Objective?
  S-DoF $=$ [rank of ■]-max{[rank of ■], [rank of ■]}

(outerbound $= 2N - N$)

The S-DoF Problem

- Q1: How to maximize the S-DoF?
- A: Choose $\mathbf{V}_i$s so that the best wiretapper listens to the the smallest space possible $\Rightarrow$ **Interference Alignment**.
- Q2: Can you formalize this?
- A:

$$
\begin{aligned}
\mathcal{V}:\quad & \\
& \min_{\mathbf{V}_1,\mathbf{V}_2} \max\left\{\operatorname{rank}\left(\blacksquare\right), \operatorname{rank}\left(\blacksquare\right)\right\} \\
\text{s.t.}\quad & \operatorname{rank}\left(\blacksquare\right) = 2N
\end{aligned}
$$

The S-DoF Problem

- Q1: How to maximize the S-DoF?
- A: Choose $\mathbf{V}_i$s so that the best wiretapper listens to the the smallest space possible $\Rightarrow$ **Interference Alignment**.
- Q2: Can you formalize this?
- A:

$$\boxed{\begin{aligned} &\mathcal{V}: \\ &\qquad \min_{\mathbf{V}_1,\mathbf{V}_2} \max\left\{\operatorname{rank}\left({\color{blue}\blacksquare}\right), \operatorname{rank}\left({\color{red}\blacksquare}\right)\right\} \\ &\text{s.t.}\ \ \operatorname{rank}\left(\blacksquare\right) = 2N \end{aligned}}$$

The S-DoF Problem

- A special class of such channels: those that achieve the S-DoF outerbound

$$\boxed{\text{S-DoF} = 2N - N}$$

- Any wiretaper's space can be squeezed into N dimensions.

The S-DoF Problem

- A special class of such channels: those that achieve the S-DoF outerbound

$$\boxed{\text{S-DoF} = 2N - N}$$

- Any wiretaper's space can be squeezed into N dimensions.

The S-DoF Problem

- A special class of such channels: those that achieve the S-DoF outerbound

$$\boxed{\text{S-DoF} = 2N - N}$$

- Any wiretaper's space can be squeezed into N dimensions.

- Minimizing the Repair BW
- Maximizing the S-DoF
- **Establishing the Connection**
- The S-DoF of SISO Multiple-Access Compound Wiretap Channel
- Extensions and Conclusions

The Connection Overview

Storage:

- 1 Desired space:

  $[\mathbf{A}_1\mathbf{R}_1\ \mathbf{A}_2\mathbf{R}_2]$: $2N \times 2N$

- 2 Harmful spaces:

  $[\mathbf{B}_1\mathbf{R}_1\ \mathbf{B}_2\mathbf{R}_2]$,
  $[\mathbf{C}_1\mathbf{R}_1\ \mathbf{C}_2\mathbf{R}_2]$: $2N \times 2N$

- 6 Coding matrices (human made):

  $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$: $2N \times 2N$

- 2 Repair matrices:

  $\mathbf{R}_i$: $2N \times N$

Wireless:

- 1 Desired space:

  $[\mathbf{H}_1\mathbf{V}_1\ \mathbf{H}_2\mathbf{V}_2]$: $2N \times 2N$

- 2 Harmful paces:

  $\left[\mathbf{H}_1^{w1}\mathbf{V}_1\ \mathbf{H}_2^{w1}\mathbf{V}_2\right]$,
  $\left[\mathbf{H}_1^{w2}\mathbf{V}_1\ \mathbf{H}_2^{w2}\mathbf{V}_2\right]$: $2N \times 2N$

- 6 Channel matrices (nature made):

  $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$: $2N \times 2N$

- 2 Beamforming matrices:

  $\mathbf{V}_i$: $2N \times N$

hmm..

- Q: What about the two optimizations $\mathcal{R}$ and $\mathcal{V}$?

The Connection Overview

Storage:

- 1 Desired space:
  $[\mathbf{A}_1\mathbf{R}_1\ \mathbf{A}_2\mathbf{R}_2]$: $2N \times 2N$
- 2 Harmful spaces:
  $[\mathbf{B}_1\mathbf{R}_1\ \mathbf{B}_2\mathbf{R}_2]$,
  $[\mathbf{C}_1\mathbf{R}_1\ \mathbf{C}_2\mathbf{R}_2]$: $2N \times 2N$
- 6 Coding matrices
  (human made):
  $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$: $2N \times 2N$
- 2 Repair matrices:
  $\mathbf{R}_i$: $2N \times N$

Wireless:

- 1 Desired space:
  $[\mathbf{H}_1\mathbf{V}_1\ \mathbf{H}_2\mathbf{V}_2]$: $2N \times 2N$
- 2 Harmful paces:
  $\left[\mathbf{H}_1^{w1}\mathbf{V}_1\ \mathbf{H}_2^{w1}\mathbf{V}_2\right]$,
  $\left[\mathbf{H}_1^{w2}\mathbf{V}_1\ \mathbf{H}_2^{w2}\mathbf{V}_2\right]$: $2N \times 2N$
- 6 Channel matrices
  (nature made):
  $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$: $2N \times 2N$
- 2 Beamforming matrices:
  $\mathbf{V}_i$: $2N \times N$

hmm..

- Q: What about the two optimizations $\mathcal{R}$ and $\mathcal{V}$?

The Connection Overview

Storage:

- 1 Desired space:

  $[\mathbf{A}_1\mathbf{R}_1 \ \mathbf{A}_2\mathbf{R}_2]$: $2N \times 2N$

- 2 Harmful spaces:

  $[\mathbf{B}_1\mathbf{R}_1 \ \mathbf{B}_2\mathbf{R}_2]$,
  $[\mathbf{C}_1\mathbf{R}_1 \ \mathbf{C}_2\mathbf{R}_2]$: $2N \times 2N$

- 6 Coding matrices (human made):

  $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$: $2N \times 2N$

- 2 Repair matrices:

  $\mathbf{R}_i$: $2N \times N$

Wireless:

- 1 Desired space:

  $[\mathbf{H}_1\mathbf{V}_1 \ \mathbf{H}_2\mathbf{V}_2]$: $2N \times 2N$

- 2 Harmful paces:

  $\left[\mathbf{H}_1^{w1}\mathbf{V}_1 \ \mathbf{H}_2^{w1}\mathbf{V}_2\right]$,
  $\left[\mathbf{H}_1^{w2}\mathbf{V}_1 \ \mathbf{H}_2^{w2}\mathbf{V}_2\right]$: $2N \times 2N$

- 6 Channel matrices (nature made):

  $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$: $2N \times 2N$

- 2 Beamforming matrices:

  $\mathbf{V}_i$: $2N \times N$

hmm..

- Q: What about the two optimizations $\mathcal{R}$ and $\mathcal{V}$?

The Connection Overview

Theorem

For any optimal storage code $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$, *minimizing the repair BW* $\equiv$ *maximizing the S-DoF of* $\mathbf{H}_i = \mathbf{A}_i, \mathbf{H}_i^{w1} = \mathbf{B}_i, \mathbf{H}_i^{w2} = \mathbf{C}_i$

Lemma

If $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$ *is a full S-DoF channel, then it is also a code with minimum repair BW for node* 1.

Lemma

If $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$ *is an optimal MDS code, then it is also a full S-DoF channel.*

The Connection Overview

Theorem

For any optimal storage code $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$, *minimizing the repair BW* $\equiv$ *maximizing the S-DoF of* $\mathbf{H}_i = \mathbf{A}_i, \mathbf{H}_i^{w1} = \mathbf{B}_i, \mathbf{H}_i^{w2} = \mathbf{C}_i$

Lemma

If $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$ *is a full S-DoF channel, then it is also a code with minimum repair BW for node* 1.

Lemma

If $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$ *is an optimal MDS code, then it is also a full S-DoF channel.*

The Connection Overview

Theorem

For any optimal storage code $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$*, minimizing the repair BW* $\equiv$ *maximizing the S-DoF of* $\mathbf{H}_i = \mathbf{A}_i, \mathbf{H}_i^{w1} = \mathbf{B}_i, \mathbf{H}_i^{w2} = \mathbf{C}_i$

Lemma

If $\mathbf{H}_i, \mathbf{H}_i^{w1}, \mathbf{H}_i^{w2}$ *is a full S-DoF channel, then it is also a code with minimum repair BW for node* 1*.*

Lemma

If $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$ *is an optimal MDS code, then it is also a full S-DoF channel.*

Sketch:

Optimal Codes:

$$\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right)+\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right)}_{\mathcal{R}} = 2\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right),\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right\}}_{\mathcal{V}} = 2N$$

Full S-DoF channels:

$$\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right),\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right\}}_{\mathcal{V}} = \frac{1}{2}\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right)+\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right)}_{\mathcal{R}} = N$$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

Sketch:

Optimal Codes:

- $$\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N} \left(\mathrm{rank}\left({\color{blue}\blacksquare}\right)+\mathrm{rank}\left({\color{red}\blacksquare}\right)\right)}_{\mathcal{R}} = 2\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\max \left\{\mathrm{rank}\left({\color{blue}\blacksquare}\right), \mathrm{rank}\left({\color{red}\blacksquare}\right)\right\}}_{\mathcal{V}} = 2N$$

Full S-DoF channels:

- $$\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\max \left\{\mathrm{rank}\left({\color{blue}\blacksquare}\right), \mathrm{rank}\left({\color{red}\blacksquare}\right)\right\}}_{\mathcal{V}} = \frac{1}{2}\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N} \left(\mathrm{rank}\left({\color{blue}\blacksquare}\right)+\mathrm{rank}\left({\color{red}\blacksquare}\right)\right)}_{\mathcal{R}} = N$$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

The Connection Overview

Sketch:

Optimal Codes:

$$\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left({\color{blue}\blacksquare}\right)+\mathrm{rank}\left({\color{red}\blacksquare}\right)\right)}_{\mathcal{R}} = 2\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left({\color{blue}\blacksquare}\right),\mathrm{rank}\left({\color{red}\blacksquare}\right)\right\}}_{\mathcal{V}} = 2N$$

Full S-DoF channels:

$$\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left({\color{blue}\blacksquare}\right),\mathrm{rank}\left({\color{red}\blacksquare}\right)\right\}}_{\mathcal{V}} = \frac{1}{2}\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left({\color{blue}\blacksquare}\right)+\mathrm{rank}\left({\color{red}\blacksquare}\right)\right)}_{\mathcal{R}} = N$$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

The Connection Overview

Sketch:

Optimal Codes:

$$\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N} \left(\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right)+\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right)}_{\mathcal{R}} = 2\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N} \max \left\{\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right),\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right\}}_{\mathcal{V}} = 2N$$

Full S-DoF channels:

$$\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N} \max \left\{\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right),\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right\}}_{\mathcal{V}} = \frac{1}{2}\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N} \left(\mathrm{rank}\left(\textcolor{blue}{\blacksquare}\right)+\mathrm{rank}\left(\textcolor{red}{\blacksquare}\right)\right)}_{\mathcal{R}} = N$$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

Sketch:

Optimal Codes:

- $\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\text{rank}(\blacksquare)=2N} \left(\text{rank}\left(\blacksquare\right) + \text{rank}\left(\blacksquare\right)\right)}_{\mathcal{R}} = 2 \underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\text{rank}(\blacksquare)=2N} \max \left\{\text{rank}\left(\blacksquare\right), \text{rank}\left(\blacksquare\right)\right\}}_{\mathcal{V}} = 2N$

Full S-DoF channels:

- $\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\text{rank}(\blacksquare)=2N} \max \left\{\text{rank}\left(\blacksquare\right), \text{rank}\left(\blacksquare\right)\right\}}_{\mathcal{V}} = \frac{1}{2} \underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\text{rank}(\blacksquare)=2N} \left(\text{rank}\left(\blacksquare\right) + \text{rank}\left(\blacksquare\right)\right)}_{\mathcal{R}} = N$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

Sketch:

Optimal Codes:

$$\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left(\blacksquare\right)+\mathrm{rank}\left(\blacksquare\right)\right)}_{\mathcal{R}}=2\underbrace{\min_{\mathbf{R}_1,\mathbf{R}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left(\blacksquare\right),\mathrm{rank}\left(\blacksquare\right)\right\}}_{\mathcal{V}}=2N$$

Full S-DoF channels:

$$\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\max\left\{\mathrm{rank}\left(\blacksquare\right),\mathrm{rank}\left(\blacksquare\right)\right\}}_{\mathcal{V}}=\frac{1}{2}\underbrace{\min_{\mathbf{V}_1,\mathbf{V}_2,\mathrm{rank}(\blacksquare)=2N}\left(\mathrm{rank}\left(\blacksquare\right)+\mathrm{rank}\left(\blacksquare\right)\right)}_{\mathcal{R}}=N$$

Solving one is solving the other

Good Codes = Good Channels

(Good Repair Matrices = Good Beamforming Matrices)

(over the same field)

Any practical examples?

The Connection Overview

Example:

- Let

$$\mathbf{A}_i = \begin{bmatrix} a_i(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots a_i(2N) \end{bmatrix}, \mathbf{B}_i = \begin{bmatrix} b_i(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots b_i(2N) \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} c_i(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots c_i(2N) \end{bmatrix}.$$

  Elements drawn iid.

- This code is *assymptotically* optimal: interference dimensions $= N'$ [CJM10], [SR10], with $\lim_{N \to \infty} \frac{N'}{N} = 1$. (Symbol Extension).

- Q: Does this map to any interesting channel?
- A: The single antenna multiple-access compound wiretap channel.

$$\mathbf{H}_i = \begin{bmatrix} h_i(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i(2N) \end{bmatrix}, \mathbf{H}_i^{w1} = \begin{bmatrix} h_i^{w1}(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{w1}(2N) \end{bmatrix}, \mathbf{H}_i^{w2} = \begin{bmatrix} h_i^{w2}(1) \ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{w2}(2N) \end{bmatrix}.$$

- normalized per user S-DoF $= \frac{2N - N'}{2N} \to \frac{1}{2}$ $\left(\frac{L-1}{L}\right.$ in general$\left.\right)$

The Connection Overview

Example:

- Let

$$\mathbf{A}_i = \begin{bmatrix} a_i(1)\dots & 0 \\ & \ddots \\ 0 & \dots a_i(2N) \end{bmatrix}, \mathbf{B}_i = \begin{bmatrix} b_i(1)\dots & 0 \\ & \ddots \\ 0 & \dots b_i(2N) \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} c_i(1)\dots & 0 \\ & \ddots \\ 0 & \dots c_i(2N) \end{bmatrix}.$$

  Elements drawn iid.

- This code is *assymptotically* optimal: interference dimensions $= N'$ [CJM10], [SR10], with $\lim_{N\to\infty} \frac{N'}{N} = 1$. (Symbol Extension).

- Q: Does this map to any interesting channel?
- A: The single antenna multiple-access compound wiretap channel.

$$\mathbf{H}_i = \begin{bmatrix} h_i(1)\dots & 0 \\ & \ddots \\ 0 & \dots h_i(2N) \end{bmatrix}, \mathbf{H}_i^{w1} = \begin{bmatrix} h_i^{w1}(1)\dots & 0 \\ & \ddots \\ 0 & \dots h_i^{w1}(2N) \end{bmatrix}, \mathbf{H}_i^{w2} = \begin{bmatrix} h_i^{w2}(1)\dots & 0 \\ & \ddots \\ 0 & \dots h_i^{w2}(2N) \end{bmatrix}.$$

- normalized per user S-DoF $= \frac{2N-N'}{2N} \to \frac{1}{2}$ $\left(\frac{L-1}{L}\right.$ in general$\left.\right)$

The Connection Overview

Example:

- Let

$$\mathbf{A}_i = \begin{bmatrix} a_i(1)\dots & 0 \\ & \ddots & \\ 0 & \dots a_i(2N) \end{bmatrix}, \mathbf{B}_i = \begin{bmatrix} b_i(1)\dots & 0 \\ & \ddots & \\ 0 & \dots b_i(2N) \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} c_i(1)\dots & 0 \\ & \ddots & \\ 0 & \dots c_i(2N) \end{bmatrix}.$$

  Elements drawn iid.

- This code is *assymptotically* optimal: interference dimensions $= N'$ [CJM10], [SR10], with $\lim_{N\to\infty} \frac{N'}{N} = 1$. (Symbol Extension).

- Q: Does this map to any interesting channel?

- A: The single antenna multiple-access compound wiretap channel.

$$\mathbf{H}_i = \begin{bmatrix} h_i(1)\dots & 0 \\ & \ddots & \\ 0 & \dots h_i(2N) \end{bmatrix}, \mathbf{H}_i^{w1} = \begin{bmatrix} h_i^{w1}(1)\dots & 0 \\ & \ddots & \\ 0 & \dots h_i^{w1}(2N) \end{bmatrix}, \mathbf{H}_i^{w2} = \begin{bmatrix} h_i^{w2}(1)\dots & 0 \\ & \ddots & \\ 0 & \dots h_i^{w2}(2N) \end{bmatrix}.$$

- normalized per user S-DoF $= \frac{2N-N'}{2N} \to \frac{1}{2}$ $\left(\frac{L-1}{L}\right.$ in general)

Example:

- Let
$$\mathbf{A}_i = \begin{bmatrix} a_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots a_i(2N) \end{bmatrix}, \mathbf{B}_i = \begin{bmatrix} b_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots b_i(2N) \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} c_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots c_i(2N) \end{bmatrix}.$$
Elements drawn iid.
- This code is *assymptotically* optimal: interference dimensions $= N'$ [CJM10], [SR10], with $\lim_{N\to\infty} \frac{N'}{N} = 1$. (Symbol Extension).

- Q: Does this map to any interesting channel?
- A: The single antenna multiple-access compound wiretap channel.

$$\mathbf{H}_i = \begin{bmatrix} h_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i(2N) \end{bmatrix}, \mathbf{H}_i^{\mathrm{w1}} = \begin{bmatrix} h_i^{\mathrm{w1}}(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{\mathrm{w1}}(2N) \end{bmatrix}, \mathbf{H}_i^{\mathrm{w2}} = \begin{bmatrix} h_i^{\mathrm{w2}}(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{\mathrm{w2}}(2N) \end{bmatrix}.$$

- normalized per user S-DoF $= \frac{2N-N'}{2N} \to \frac{1}{2}$ ($\frac{L-1}{L}$ in general)

The Connection Overview

Example:

- Let

$$\mathbf{A}_i = \begin{bmatrix} a_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots a_i(2N) \end{bmatrix}, \mathbf{B}_i = \begin{bmatrix} b_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots b_i(2N) \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} c_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots c_i(2N) \end{bmatrix}.$$

  Elements drawn iid.

- This code is *assymptotically* optimal: interference dimensions $= N'$ [CJM10], [SR10], with $\lim_{N\to\infty} \frac{N'}{N} = 1$. (Symbol Extension).

- Q: Does this map to any interesting channel?
- A: The single antenna multiple-access compound wiretap channel.

$$\mathbf{H}_i = \begin{bmatrix} h_i(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i(2N) \end{bmatrix}, \mathbf{H}_i^{w1} = \begin{bmatrix} h_i^{w1}(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{w1}(2N) \end{bmatrix}, \mathbf{H}_i^{w2} = \begin{bmatrix} h_i^{w2}(1)\ldots & 0 \\ & \ddots & \\ 0 & \ldots h_i^{w2}(2N) \end{bmatrix}.$$

- normalized per user S-DoF $= \frac{2N-N'}{2N} \longrightarrow \frac{1}{2}$ ($\frac{L-1}{L}$ in general)

The Connection Overview

- For codes and channels that are not that good we use

$$\frac{1}{n}\sum_{i=1}^{n} r_i \leq \max_i r_i \leq \sum_{i=1}^{n} r_i \leq n \max_i r_i$$

to derive bounds.

Conclusions

- IA is used in both the Repair and S-DoF maximization problems.
- We can formulate them as Rank Constrained Rank Minimizations,
- and establish a connection between the two, with mappings and reductions.
- Then, using a repair code we characterized the S-DoF of the SISO muliple-access compound wiretap channel.

Thank you!