Graphs and Algebra in Modern Communication.

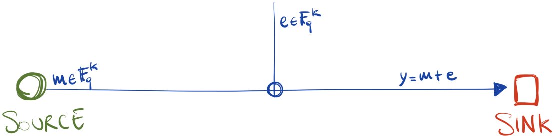
Felice Manganiello
School of Math and Stat Sciences @ Clemson University
Cybersecurity Research Lab @ Ryerson University

May 26, 2020

Joint work with
Kschischang (UofT), **Ravagnani (TU/e)**, *Savary (Clemson)*
Kai (UMichigan), Pedro (UMaryland), Paige (U of Mary Washington),
Kimberly (Bowdoin College) and Nathan (Haverford College)

Partially funded by NSF Grant No. DMS:1547399.

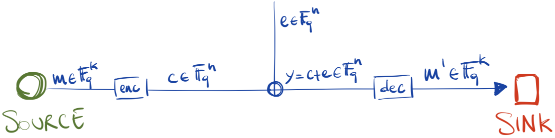
Noisy-Channel Coding Theorem (1948)



Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

"Any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can always be attained with an arbitrarily small probability of error."

Noisy-Channel Coding Theorem (1948)

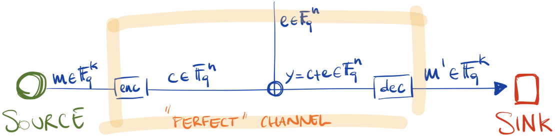


Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

"Any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can always be attained with an arbitrarily small probability of error."

Solved: Turbo codes (LTE networks), Polar & spatially-coupled LDPC codes (5G networks)

Noisy-Channel Coding Theorem (1948)



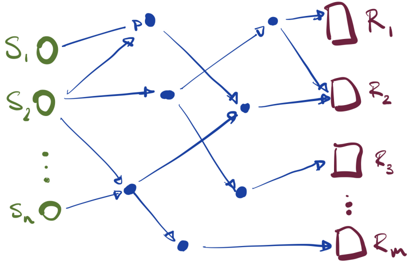
Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

"Any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can always be attained with an arbitrarily small probability of error."

Solved: Turbo codes (LTE networks), Polar & spatially-coupled LDPC codes (5G networks)

Networks - a graph perspective

A network is a *directed acyclic graph* $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{R}, \mathbb{F}_q)$.



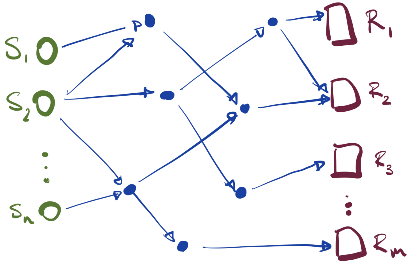
- Sources: nodes with no incoming edges, $\mathcal{S} \subsetneq \mathcal{V}$.
- Sinks: nodes with no outgoing edges, $\mathcal{R} \subsetneq \mathcal{V}$.
- Edges represent perfect unit capacity channels.
- each sink $R \in \mathcal{R}$ demands messages from $D_R \subseteq \mathcal{S}$.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

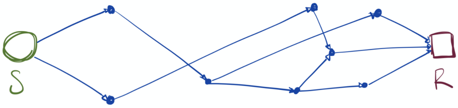
Networks - a graph perspective

A network is a *directed acyclic graph* $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{R}, \mathbb{F}_q)$.



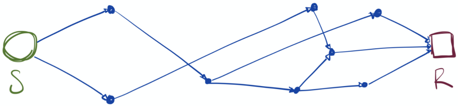
- *Unicast Problem*: $|\mathcal{S}| = |\mathcal{R}| = 1$ and $D_R = \mathcal{S}$.
- *Multicast Problem*: $|\mathcal{R}| \geq 1$ and $D_R = \mathcal{S}$ for all $R \in \mathcal{R}$.
- *Multiple Unicast problem*: $\mathcal{S} = \{S_1, \ldots, S_n\}$, $\mathcal{R} = \{R_1, \ldots, R_n\}$, and $D_{R_i} = \{S_i\}$.

Unicast Network



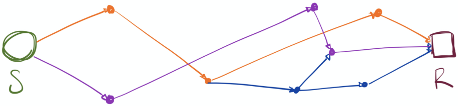
- Communication rate: $\rho \leq \mathrm{mincut}(S, R)$.

Unicast Network



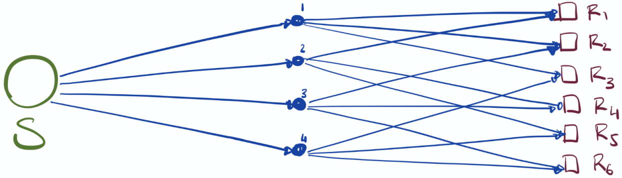
- Communication rate: $\rho \leq \mathrm{mincut}(S, R)$.
- Menger's Theorem: $\mathrm{mincut}(S, R) =$ maximum number of pairwise edge–disjoint paths.

Unicast Network

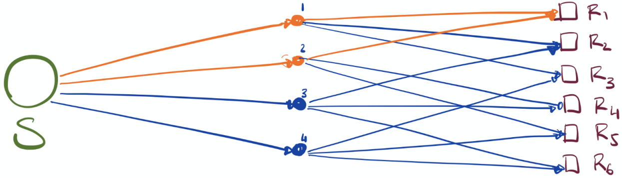


- Communication rate: $\rho \leq \mathrm{mincut}(S, R)$.
- Menger's Theorem: $\mathrm{mincut}(S, R) =$ maximum number of pairwise edge–disjoint paths.
- Routing maximizes R.

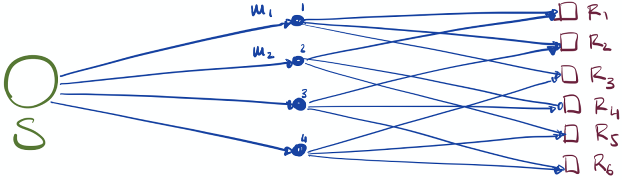
Multicast network [Li et al., 2003, Koetter and Medard, 2003]



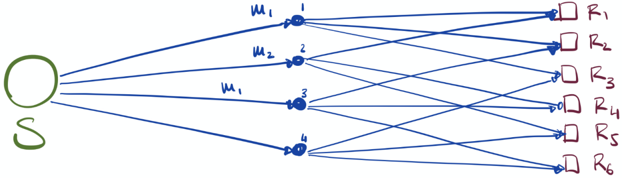
Multicast network [Li et al., 2003, Koetter and Medard, 2003]



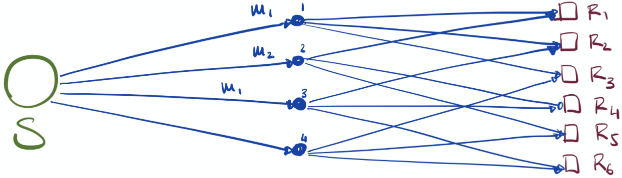
Multicast network [Li et al., 2003, Koetter and Medard, 2003]



Multicast network [Li et al., 2003, Koetter and Medard, 2003]



Multicast network [Li et al., 2003, Koetter and Medard, 2003]



Theorem (Linear Network Multicasting Theorem)

Let $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{R}, \mathbb{F}_q)$. *A multicast rate of*

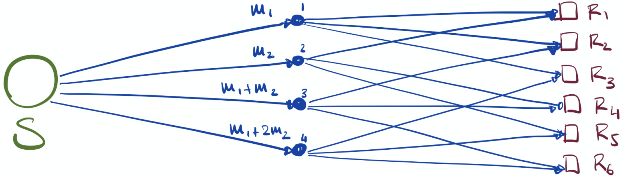
$$\min_{R \in \mathcal{R}} \mathrm{mincut}(\mathcal{S}, R)$$

is achievable, for sufficiently large q, with linear network coding.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Multicast network [Li et al., 2003, Koetter and Medard, 2003]



Theorem (Linear Network Multicasting Theorem)

Let $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{R}, \mathbb{F}_q)$*. A multicast rate of*

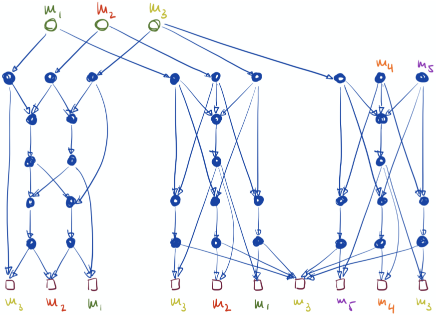
$$\min_{R \in \mathcal{R}} \mathrm{mincut}(\mathcal{S}, R)$$

is achievable, for sufficiently large q, with linear network coding.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Insufficiency of LNC [Dougherty et al., 2005]



Theorem

There exists an solvable network that has no linear solution over any finite field and any vector dimension.

1. Introduction

2. Interference Networks
   - Definition
   - Multiple Unicast network
   - Linear Achievability and complexity

3. Achievability bounds for Multiple Unicast Networks
   - Lower Bound
   - Upper Bounds

4. Conclusions

Networks and Interference

"Interference is a major impairment to the reliable communication in multi-user wireless networks, due to the broadcast and superposition nature of wireless medium." [Zhao et al., 2016]

Networks and Interference

"Interference is a major impairment to the reliable communication in multi-user wireless networks, due to the broadcast and superposition nature of wireless medium." [Zhao et al., 2016]

Let $\mathcal{N}$ be a network with $\mathcal{S}$ sources set and $\mathcal{R}$ receivers set. A network has interference if

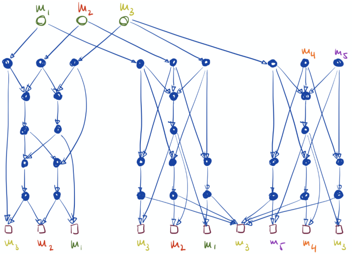
- $D_R \neq \mathcal{S}$ for some $R \in \mathcal{R}$
- for some $R \in \mathcal{R}$ there is a paths between $S \notin D_R$ and R.

Networks and Interference

"Interference is a major impairment to the reliable communication in multi-user wireless networks, due to the broadcast and superposition nature of wireless medium." [Zhao et al., 2016]

Let $\mathcal{N}$ be a network with $\mathcal{S}$ sources set and $\mathcal{R}$ receivers set. A network has interference if

- $D_R \neq \mathcal{S}$ for some $R \in \mathcal{R}$
- for some $R \in \mathcal{R}$ there is a paths between $S \notin D_R$ and R.



Multiple Unicast network

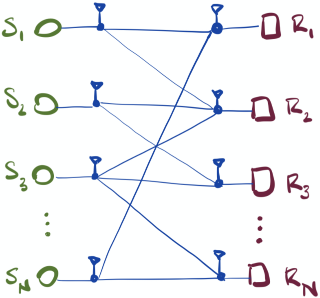
Definition

A multiple unicast network is a network $\mathcal{N}$ such that $|\mathcal{S}| = |\mathcal{R}|$ and $D_{R_i} = \{S_i\}$ for $i = 1, \ldots, |\mathcal{S}|$.

Multiple Unicast network

Definition

A multiple unicast network is a network $\mathcal{N}$ such that $|\mathcal{S}| = |\mathcal{R}|$ and $D_{R_i} = \{S_i\}$ for $i = 1, \ldots, |\mathcal{S}|$.

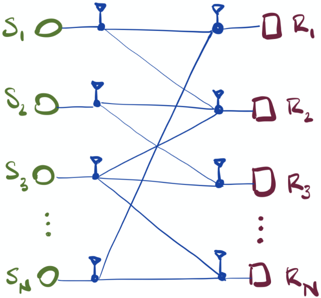


Communication strategy:

Multiple Unicast network

Definition

A multiple unicast network is a network $\mathcal{N}$ such that $|\mathcal{S}| = |\mathcal{R}|$ and $D_{R_i} = \{S_i\}$ for $i = 1, \ldots, |\mathcal{S}|$.



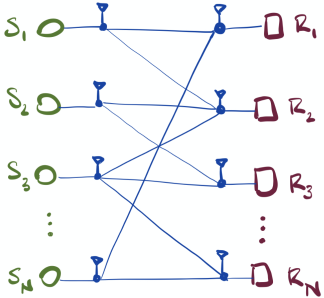
Communication strategy:

- 1 round

Multiple Unicast network

Definition

A multiple unicast network is a network $\mathcal{N}$ such that $|\mathcal{S}| = |\mathcal{R}|$ and $D_{R_i} = \{S_i\}$ for $i = 1, \ldots, |\mathcal{S}|$.



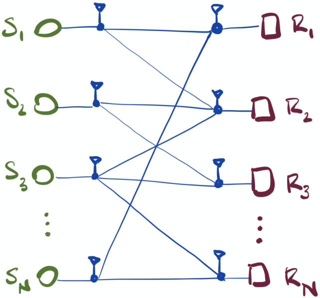
Communication strategy:

- 1 round $\rightarrow$ no interference-free communication possible.

Multiple Unicast network

Definition

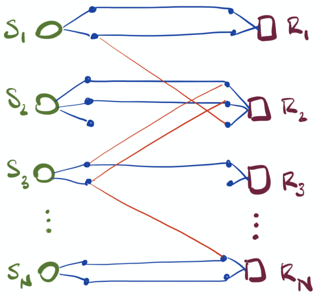
A multiple unicast network is a network $\mathcal{N}$ such that $|\mathcal{S}| = |\mathcal{R}|$ and $D_{R_i} = \{S_i\}$ for $i = 1, \ldots, |\mathcal{S}|$.



Communication strategy:

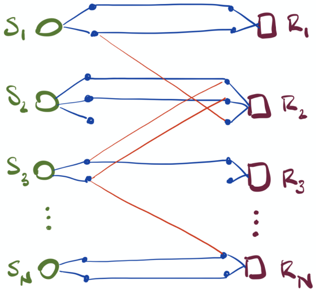
- 1 round $\rightarrow$ no interference-free communication possible.
- multiple rounds $\rightarrow$ time sharing.

Multiple Unicast network (cont'd)



Communication strategy:

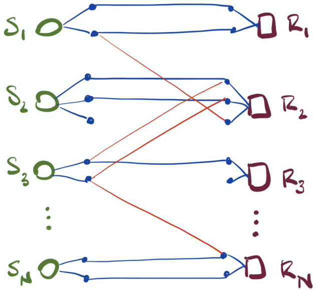
Multiple Unicast network (cont'd)



Communication strategy:

- multiple rounds $\rightarrow$ time sharing.

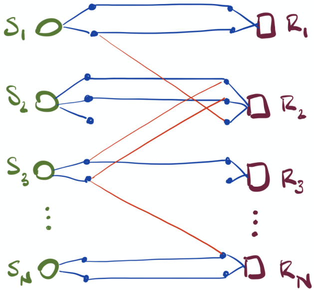
Multiple Unicast network (cont'd)



Communication strategy:

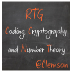
- multiple rounds → time sharing.
- 1 round →

Multiple Unicast network (cont'd)



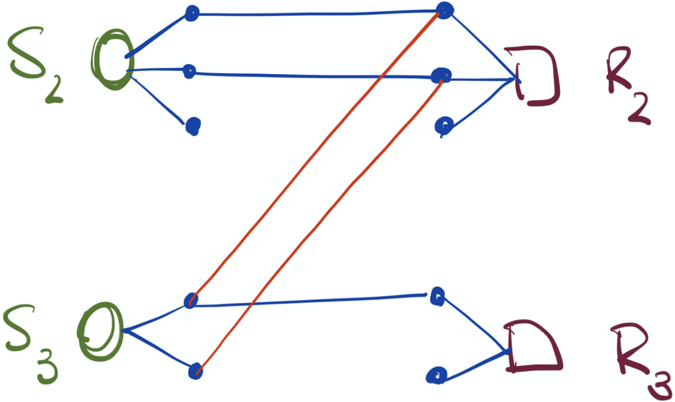
Communication strategy:

- multiple rounds $\to$ time sharing.
- 1 round $\to$ *interference alignment*, meaning use of subspaces to communicate without interference
- original paper [Cadambe and Jafar, 2008].

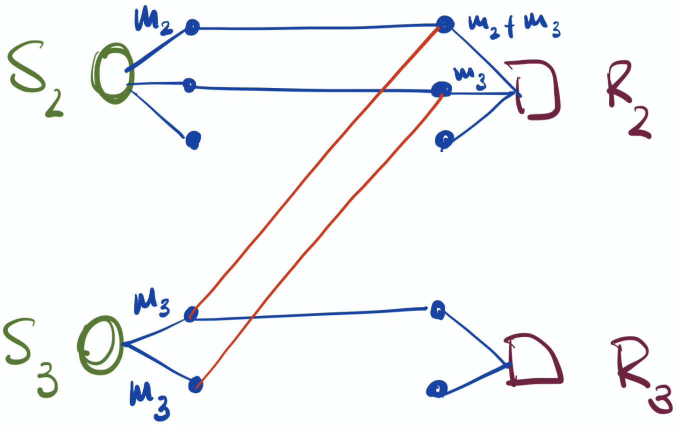


CLEMSON UNIVERSITY

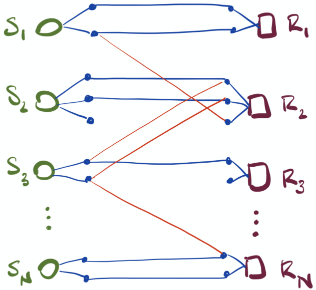
Multiple Unicast network (cont'd)



Multiple Unicast network (cont'd)



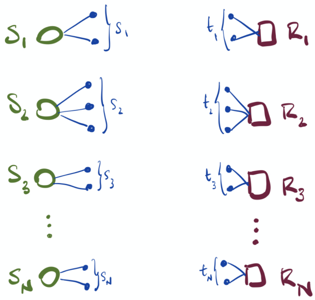
Multiple Unicast network (cont'd)



Communication strategy:

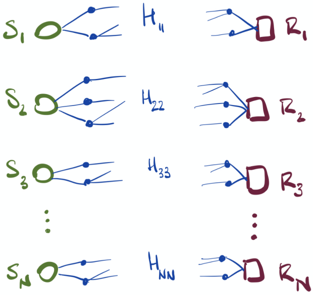
- multiple rounds → time sharing.
- 1 round → *interference alignment*, meaning use of subspaces to communicate without interference

Multiple Unicast network - Notation



- s_i number of antennas available to source S_i and $s = \sum_{i=1}^{N} s_i$.
- t_i number of antennas available to source R_i and $t = \sum_{i=1}^{N} t_i$.

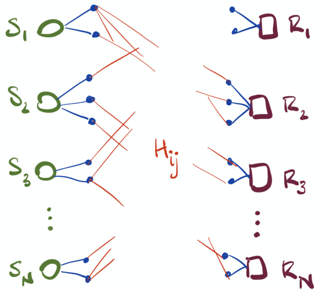
Multiple Unicast network - Notation



- s_i number of antennas available to source S_i and $s = \sum_{i=1}^{N} s_i$.
- t_i number of antennas available to source R_i and $t = \sum_{i=1}^{N} t_i$.
- The adjacency matrix $H \in \{0,1\}^{t \times s}$,

$$H = \begin{pmatrix} H_{11} & & \\ & H_{22} & \\ & & H_{NN} \end{pmatrix}$$

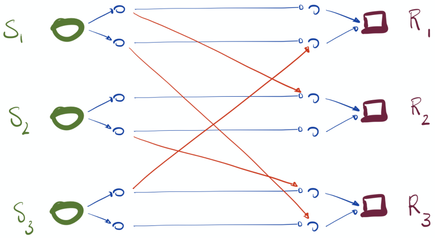
Multiple Unicast network - Notation



- s_i number of antennas available to source S_i and $s = \sum_{i=1}^{N} s_i$.
- t_i number of antennas available to source R_i and $t = \sum_{i=1}^{N} t_i$.
- The adjacency matrix $H \in \{0,1\}^{t \times s}$,

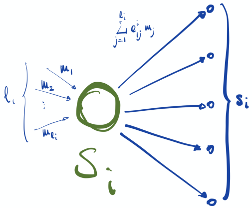
$$H = \begin{pmatrix} H_{11} & H_{12} & \dots & H_{1N} \\ H_{21} & H_{22} & \dots & H_{2N} \\ \vdots & \vdots & & \vdots \\ H_{N1} & H_{N2} & \dots & H_{NN} \end{pmatrix}$$

Example



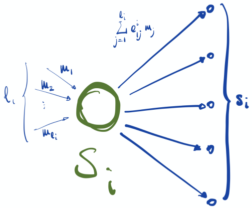
$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Linear Encoders and Decoders



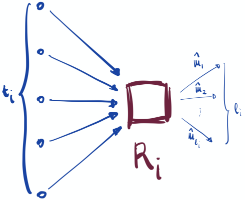
$$E = \begin{pmatrix} E_1 & 0 & \dots & 0 \\ 0 & E_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & E_N \end{pmatrix}$$

Linear Encoders and Decoders



$$E = \begin{pmatrix} E_1 & 0 & \dots & 0 \\ 0 & E_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & E_N \end{pmatrix}$$

$$D = \begin{pmatrix} D_1 & 0 & \dots & 0 \\ 0 & D_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & D_N \end{pmatrix}$$



Linear Network Communication

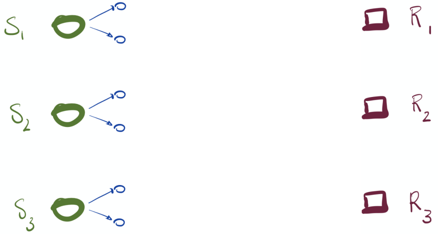
$$\begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} \qquad \overset{j \neq i}{} \qquad \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix}$$

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

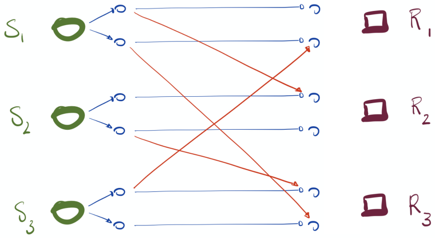
Linear Network Communication

$$E_i \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} \qquad j \neq i \qquad E_j \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix}$$



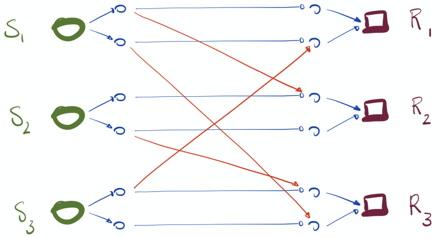
Linear Network Communication

$$H_{ii}E_i \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} + \sum_{j \neq i} H_{ij}E_j \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix}$$



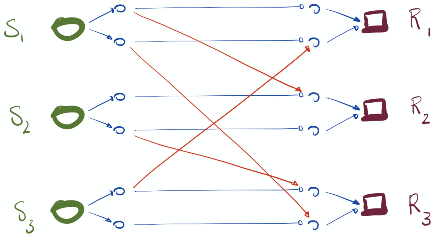
Linear Network Communication

$$D_i H_{ii} E_i \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} + \sum_{j \neq i} D_i H_{ij} E_j \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix}$$



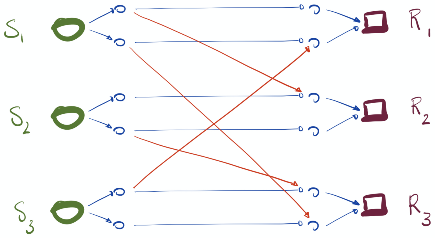
Linear Network Communication

$$\begin{pmatrix} \hat{m}_{i,1} \\ \vdots \\ \hat{m}_{i,\ell_i} \end{pmatrix} = D_i H_{ii} E_i \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} + \sum_{j \neq i} D_i H_{ij} E_j \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix}$$



Linear Network Communication

$$\begin{pmatrix} \hat{m}_{i,1} \\ \vdots \\ \hat{m}_{i,\ell_i} \end{pmatrix} = D_i H_{ii} E_i \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix} + \sum_{j \neq i} D_i H_{ij} E_j \begin{pmatrix} m_{j,1} \\ \vdots \\ m_{j,\ell_j} \end{pmatrix} = \begin{pmatrix} m_{i,1} \\ \vdots \\ m_{i,\ell_i} \end{pmatrix}$$



Linear Achievability of Multiple Unicast networks

Definition

A network $\mathcal{N}$ is linearly achievable for $\rho = (\rho_1, \dots, \rho_N) \in \mathbb{Z}^N$, or simply ρ-linearly achievable, if there exist two matrices D, E (with entries in $\mathbb{F}_q$) such that

$$D_i H_{ij} E_j = 0 \text{ and } \operatorname{rank}(D_i H_{ii} E_i) = \rho_i.$$

- $D_i H_{ii} E_i$ is a $\ell_i \times \ell_i$ matrix.
- wlog D_i can be chosen to be in RCEF and messages are sent at pivot positions.

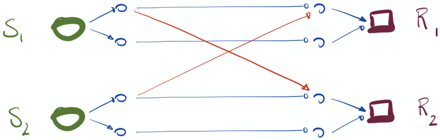
$$D_i H_{ii} E_i \begin{pmatrix} m_1 \\ 0 \\ m_3 \\ \vdots \\ m_{\rho_i} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \star & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} m_1 \\ 0 \\ m_3 \\ \vdots \\ m_{\rho_i} \end{pmatrix} = \begin{pmatrix} m_1 \\ \star \\ m_3 \\ \vdots \\ m_{\rho_i} \end{pmatrix}$$

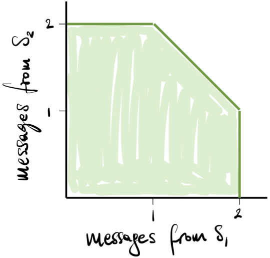
Linear Achievability Region

Definition

The *linear achievability region* of network $\mathcal{N}$, denoted $\mathrm{Lin}(\mathcal{N})$, is the subset of $\mathbb{R}^N$ for which $\mathcal{N}$ is ρ-linearly achievable.

$$H = \begin{pmatrix} 1 & 0 & \color{red}{1} & 0 \\ 0 & 1 & 0 & 0 \\ \color{red}{1} & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$





Algebraic model

We represent a network $\mathcal{N}$ by matrices with

$$DHE = \begin{pmatrix} D_1 H_{11} E_1 & \dots & D_1 H_{1N} E_N \\ D_2 H_{21} E_1 & \dots & D_2 H_{2N} E_N \\ \vdots & \ddots & \vdots \\ D_N H_{N1} E_1 & \dots & D_N H_{NN} E_N \end{pmatrix}$$

where $E \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{s \times \ell\}}$ and $D \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{\ell \times t\}}$.

Algebraic model

We represent a network $\mathcal{N}$ by matrices with

$$DHE = \begin{pmatrix} D_1 H_{11} E_1 & \dots & D_1 H_{1N} E_N \\ D_2 H_{21} E_1 & \dots & D_2 H_{2N} E_N \\ \vdots & \ddots & \vdots \\ D_N H_{N1} E_1 & \dots & D_N H_{NN} E_N \end{pmatrix}$$

where $E \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{s \times \ell\}}$ and $D \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{\ell \times t\}}$.

Optimization problem. Find matrices E, D such that

Algebraic model

We represent a network $\mathcal{N}$ by matrices with

$$DHE = \begin{pmatrix} D_1 H_{11} E_1 & \dots & D_1 H_{1N} E_N \\ D_2 H_{21} E_1 & \dots & D_2 H_{2N} E_N \\ \vdots & \ddots & \vdots \\ D_N H_{N1} E_1 & \dots & D_N H_{NN} E_N \end{pmatrix}$$

where $E \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{s\times\ell\}}$ and $D \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{\ell\times t\}}$.

Optimization problem. Find matrices E, D such that

- $D_i H_{ij} E_j = 0$

Algebraic model

We represent a network $\mathcal{N}$ by matrices with

$$DHE = \begin{pmatrix} D_1 H_{11} E_1 & \dots & D_1 H_{1N} E_N \\ D_2 H_{21} E_1 & \dots & D_2 H_{2N} E_N \\ \vdots & \ddots & \vdots \\ D_N H_{N1} E_1 & \dots & D_N H_{NN} E_N \end{pmatrix}$$

where $E \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{s \times \ell\}}$ and $D \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{\ell \times t\}}$.

Optimization problem. Find matrices E, D such that

- $D_i H_{ij} E_j = 0 \quad \longrightarrow \quad$ homogeneous bilinear system.

Algebraic model

We represent a network $\mathcal{N}$ by matrices with

$$DHE = \begin{pmatrix} D_1 H_{11} E_1 & \dots & D_1 H_{1N} E_N \\ D_2 H_{21} E_1 & \dots & D_2 H_{2N} E_N \\ \vdots & \ddots & \vdots \\ D_N H_{N1} E_1 & \dots & D_N H_{NN} E_N \end{pmatrix}$$

where $E \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{s \times \ell\}}$ and $D \in \mathbb{F}_q[\underline{e}, \underline{d}]^{\{\ell \times t\}}$.

Optimization problem. Find matrices E, D such that

- $D_i H_{ij} E_j = 0 \quad \longrightarrow \quad$ homogeneous bilinear system.
- rank $D_i H_{ii} E_i$ is maximal.

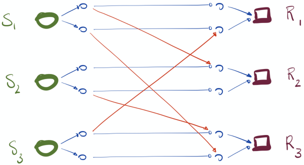
RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

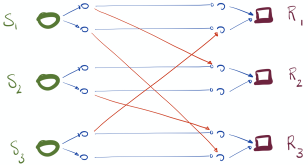
Some preliminary results

Lemma

If $\mathcal{N}$ is ρ-linearly achievable then
$\rho_i \leq \text{rank } H_{ii} = r_i$.



Some preliminary results



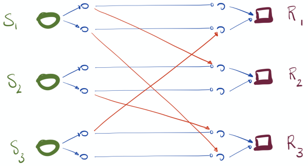
Lemma

If $\mathcal{N}$ is ρ-linearly achievable then $\rho_i \leq \text{rank } H_{ii} = r_i$.

Lemma

Let $\mathcal{N}$ be such that $t_i = s_i = r_i = \ell_i$ for all $1 \leq i \leq N$. Then $\mathcal{N}$ is ℓ-linearly achievable for $\ell = (\ell_1, \ldots, \ell_N)$ only if D, $H$and E are fullrank.

Some preliminary results



Lemma

If $\mathcal{N}$ is ρ-linearly achievable then
$\rho_i \leq \text{rank } H_{ii} = r_i$.

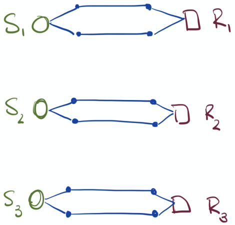
Lemma

Let $\mathcal{N}$ be such that $t_i = s_i = r_i = \ell_i$ for all $1 \leq i \leq N$. Then $\mathcal{N}$ is ℓ-linearly achievable for $\ell = (\ell_1, \ldots, \ell_N)$ only if D, $H$and E are fullrank.

Theorem

Let $\mathcal{N}$ be such that $t_i = s_i = r_i = \ell_i$ for all $1 \leq i \leq N$. If $\mathcal{N}$ has interference then $\mathcal{N}$ is not linearly achievable for ℓ (for all finite fields).

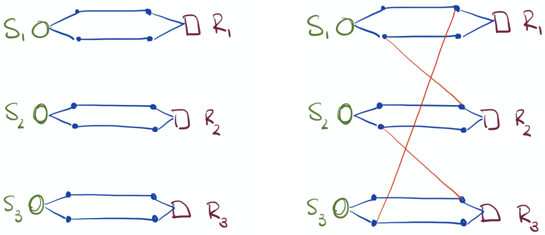
Lower achievability bound



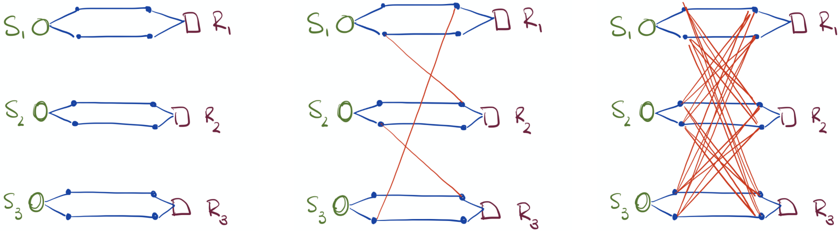
RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Lower achievability bound



Lower achievability bound



Sufficient condition for solvability

$$H = \begin{pmatrix} H_{11} & H_{12} & \dots & H_{1N} \\ H_{21} & H_{22} & \dots & H_{2N} \\ \vdots & & & \vdots \\ H_{N1} & H_{N2} & \dots & H_{NN} \end{pmatrix}$$

Definition

We call rank of interference the value $o_i := rank(H_{ij} \mid j \neq i)$.

Sufficient condition for solvability

$$H = \begin{pmatrix} H_{11} & H_{12} & \dots & H_{1N} \\ H_{21} & H_{22} & \dots & H_{2N} \\ \vdots & & & \vdots \\ H_{N1} & H_{N2} & \dots & H_{NN} \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Definition

We call rank of interference the value $o_i := rank(H_{ij} \mid j \neq i)$.

$$o_1 = 1, \; o_2 = 1, \; o_3 = 2$$

Theorem

A network $\mathcal{N}$ is $(r_1 - o_1, \dots, r_N - o_N)$-linearly achievable and matrices E and D can be computed using Gaussian elimination 2N times.

$\mathcal{N}$ is $(1, 1, 0)$-linearly achievable.

CLEMSON UNIVERSITY

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker\left(H_{ij} \mid j \neq i\right)$.

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker\left(H_{ij} \mid j \neq i\right)$.
- $(H_{ij} \mid j \neq i)$ is a matrix with t_i rows and rank o_i.

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker\left(H_{ij} \mid j \neq i\right)$.
- $\left(H_{ij} \mid j \neq i\right)$ is a matrix with t_i rows and rank o_i.
- $\dim \ell\ker\left(H_{ij} \mid j \neq i\right)$ is $t_i - o_i$.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker\left(H_{ij} \mid j \neq i\right)$.
- $(H_{ij} \mid j \neq i)$ is a matrix with t_i rows and rank o_i.
- $\dim \ell\ker\left(H_{ij} \mid j \neq i\right)$ is $t_i - o_i$.
- Choose the rows of D_i to span the $\ell\ker\left(H_{ij} \mid j \neq i\right)$.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker\left(H_{ij} \mid j \neq i\right)$.
- $(H_{ij} \mid j \neq i)$ is a matrix with t_i rows and rank o_i.
- $\dim \ell\ker\left(H_{ij} \mid j \neq i\right)$ is $t_i - o_i$.
- Choose the rows of D_i to span the $\ell\ker\left(H_{ij} \mid j \neq i\right)$.
- Without loss of generality H_{ii} is a partial identity of rank r_i.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Proof of the lower bound

Denote by $\ell\text{ker}(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\text{ker}\,(H_{ij} \mid j \neq i)$.
- $(H_{ij} \mid j \neq i)$ is a matrix with t_i rows and rank o_i.
- $\dim \ell\text{ker}\,(H_{ij} \mid j \neq i)$ is $t_i - o_i$.
- Choose the rows of D_i to span the $\ell\text{ker}\,(H_{ij} \mid j \neq i)$.
- Without loss of generality H_{ii} is a partial identity of rank r_i.
- $\text{rank}\, D_i H_{ii} \geq (t_i - o_i) - (t_i - r_i) = r_i - o_i$.

Proof of the lower bound

Denote by $\ell\ker(H_{ij} \mid j \neq i)$ be the left kernel of $(H_{ij} \mid j \neq i)$.

- $D_i H_{ij} = 0$ if and only if the rows of D_i are contained in $\ell\ker(H_{ij} \mid j \neq i)$.
- $(H_{ij} \mid j \neq i)$ is a matrix with t_i rows and rank o_i.
- $\dim \ell\ker(H_{ij} \mid j \neq i)$ is $t_i - o_i$.
- Choose the rows of D_i to span the $\ell\ker(H_{ij} \mid j \neq i)$.

- Without loss of generality H_{ii} is a partial identity of rank r_i.
- $\operatorname{rank} D_i H_{ii} \geq (t_i - o_i) - (t_i - r_i) = r_i - o_i$.
- Let E_i be any invertible matrix, then $\operatorname{rank} D_i H_{ii} E_i \geq r_i - o_i$.

Encoding-Dependent Linear Achievability

Theorem

A network $\mathcal{N}$ is $\rho = (\rho_1, \ldots, \rho_n)$-linearly achievable if and only if there exist $E_1, \ldots, E_n$ such that for all $i \in [N]$ if holds that

$$\rho_i \leq \dim \,{}^{\ell}\mathrm{ker}(H_{ij}E_j \mid j \neq i) / {}^{\ell}\mathrm{ker}(H_{ij}E_j \mid \forall\, j).$$

Moreover the bound is always tight.

Encoding-Dependent Linear Achievability

Theorem

A network $\mathcal{N}$ is $\rho = (\rho_1, \ldots, \rho_n)$-linearly achievable if and only if there exist $E_1, \ldots, E_n$ such that for all $i \in [N]$ if holds that

$$\rho_i \leq \dim {}^{\ell\mathrm{ker}(H_{ij}E_j \mid j \neq i)}/_{\ell\mathrm{ker}(H_{ij}E_j \mid \forall j)}.$$

Moreover the bound is always tight.

- Let $V_i = {}^{\ell\mathrm{ker}(H_{ij}E_j \mid j \neq i)}/_{\ell\mathrm{ker}(H_{ij}E_j \mid \forall j)}$

Encoding-Dependent Linear Achievability

Theorem

A network $\mathcal{N}$ is $\rho = (\rho_1, \ldots, \rho_n)$-linearly achievable if and only if there exist $E_1, \ldots, E_n$ such that for all $i \in [N]$ if holds that

$$\rho_i \leq \dim \; {}^{\ell\ker(H_{ij}E_j \mid j \neq i)} \big/ {}_{\ell\ker(H_{ij}E_j \mid \forall\, j)}.$$

Moreover the bound is always tight.

- Let $V_i = {}^{\ell\ker(H_{ij}E_j \mid j \neq i)} \big/ {}_{\ell\ker(H_{ij}E_j \mid \forall\, j)}$
- If D_i is such that $D_i H_{ij} E_j = 0$, then the rows of D_i belong to $\ell\ker(H_{ij}E_j \mid j \neq i)$.

Encoding-Dependent Linear Achievability

Theorem

A network $\mathcal{N}$ is $\rho = (\rho_1, \ldots, \rho_n)$-linearly achievable if and only if there exist $E_1, \ldots, E_n$ such that for all $i \in [N]$ if holds that

$$\rho_i \leq \dim {}^{\ell\ker(H_{ij}E_j \mid j \neq i)}/_{\ell\ker(H_{ij}E_j \mid \forall j)}.$$

Moreover the bound is always tight.

- Let $V_i = {}^{\ell\ker(H_{ij}E_j \mid j \neq i)}/_{\ell\ker(H_{ij}E_j \mid \forall j)}$
- If D_i is such that $D_i H_{ij} E_j = 0$, then the rows of D_i belong to $\ell\ker(H_{ij}E_j \mid j \neq i)$.
- Let $v_{i,1}, \ldots, v_{i,\ell_i}$ be the rows of D_i, then

$$\begin{aligned}\operatorname{rank} D_i H_{ii} E_i &= \dim\langle v_{i,1} H_{ii} E_i, \ldots, v_{i,\ell_i} H_{ii} E_i \rangle \\ &\leq \dim {}^{\ell\ker(H_{ij}E_j \mid j \neq i)}/_{\ell\ker(H_{ij}E_j \mid \forall j)}\end{aligned}$$

Encoding-Dependent Linear Achievability

Theorem

A network $\mathcal{N}$ is $\rho = (\rho_1, \ldots, \rho_n)$-linearly achievable if and only if there exist $E_1, \ldots, E_n$ such that for all $i \in [N]$ if holds that

$$\rho_i \leq \dim \,^{\ell\ker(H_{ij}E_j \mid j \neq i)}\!/_{\ell\ker(H_{ij}E_j \mid \forall\, j)}.$$

Moreover the bound is always tight.

- Let $V_i = \,^{\ell\ker(H_{ij}E_j \mid j \neq i)}\!/_{\ell\ker(H_{ij}E_j \mid \forall\, j)}$
- If D_i is such that $D_i H_{ij} E_j = 0$, then the rows of D_i belong to $\ell\ker(H_{ij}E_j \mid j \neq i)$.
- Let $v_{i,1}, \ldots, v_{i,\ell_i}$ be the rows of D_i, then

$$\begin{aligned}\operatorname{rank} D_i H_{ii} E_i &= \dim\langle v_{i,1} H_{ii} E_i, \ldots, v_{i,\ell_i} H_{ii} E_i \rangle \\ &\leq \dim \,^{\ell\ker(H_{ij}E_j \mid j \neq i)}\!/_{\ell\ker(H_{ij}E_j \mid \forall\, j)}\end{aligned}$$

- $\operatorname{rank} D_i H_{ii} E_i = \dim V_i$ iff $\{[v_{i,1}], \ldots, [v_{i,\ell_i}]\}$ spans V_i.

Example

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

Example

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Example

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H_{31}E_1 = 0 \qquad H_{32}E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad H_{33}E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\ell\ker H_{31}E_1 = \mathbb{F}_q^2 \qquad \ell\ker H_{32}E_2 = \langle (0,1) \rangle \qquad \ell\ker H_{33}E_2 = \langle (1,0) \rangle$$

Example

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H_{31}E_1 = 0 \qquad H_{32}E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad H_{33}E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\ell\ker H_{31}E_1 = \mathbb{F}_q^2 \qquad \ell\ker H_{32}E_2 = \langle(0,1)\rangle \qquad \ell\ker H_{33}E_2 = \langle(1,0)\rangle$$

$$\rho_3 = \dim {}^{\ell\ker(H_{3j}E_j \mid j \neq 3)}/_{\ell\ker(H_{3j}E_j \mid \forall j)} = \dim {}^{\langle(0,1)\rangle}/_{\{0\}} = 1$$

Example

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H_{31}E_1 = 0 \qquad H_{32}E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad H_{33}E_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\ell\ker H_{31}E_1 = \mathbb{F}_q^2 \qquad \ell\ker H_{32}E_2 = \langle (0,1) \rangle \qquad \ell\ker H_{33}E_2 = \langle (1,0) \rangle$$

$$\rho_3 = \dim {}^{\ell\ker(H_{3j}E_j \mid j \neq 3)}/_{\ell\ker(H_{3j}E_j \mid \forall j)} = \dim {}^{\langle (0,1) \rangle}/_{\{0\}} = 1$$

$$D_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Conclusions

Future projects

- Find Lin($\mathcal{N}$) for all multiple unicast networks.
- Find good algorithmic methods to solve the optimization problem.
- Prove that linearity is actually optimal for the explained multiple unicast networks.
- Generalize these results to other interference networks

Conclusions

Future projects

- Find Lin($\mathcal{N}$) for all multiple unicast networks.
- Find good algorithmic methods to solve the optimization problem.
- Prove that linearity is actually optimal for the explained multiple unicast networks.
- Generalize these results to other interference networks

Thank you.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

References

Cadambe, V. R. and Jafar, S. A. (2008).
Interference alignment and degrees of freedom of the k-user interference channel.
IEEE Transactions on Information Theory, 54(8):3425–3441.

Dougherty, R., Freiling, C., and Zeger, K. (2005).
Insufficiency of linear coding in network information flow.
IEEE Transactions on Information Theory, 51(8):2745–2759.

Koetter, R. and Medard, M. (2003).
An algebraic approach to network coding.
IEEE/ACM Transactions on Networking, 11(5):782–795.

Li, S. . R., Yeung, R. W., and Ning Cai (2003).
Linear network coding.
IEEE Transactions on Information Theory, 49(2):371–381.

Zhao, N., Yu, F. R., Jin, M., Yan, Q., and Leung, V. C. M. (2016).
Interference alignment and its applications: A survey, research issues, and challenges.
IEEE Communications Surveys Tutorials, 18(3):1779–1803.