Network Coding and the Rank Metric

Alberto Ravagnani

University College Dublin

ICERM, Nov. 2018

Outline

1. Network coding
2. Rank-metric codes and q-polymatroids

Outline

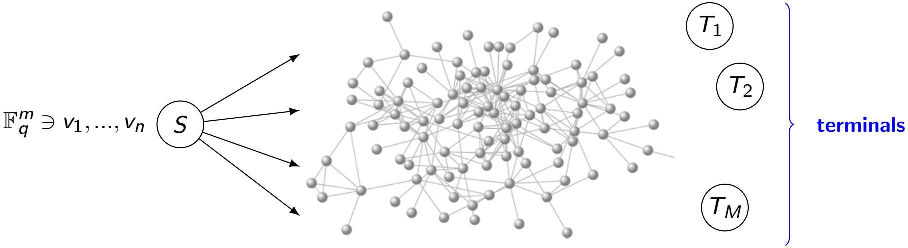
1. Network coding

2. Rank-metric codes and q-polymatroids

What is network coding about?

Network coding: data transmission over networks (streaming, patches distribution, ...)

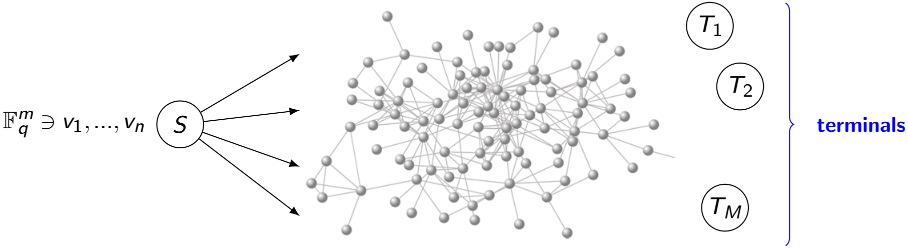
Network coding: data transmission over networks (streaming, patches distribution, ...)



- One source S attempts to transmit messages $v_1, \dots, v_n \in \mathbb{F}_q^m$.
- The terminals demand **all** the messages (multicast).

What is network coding about?

Network coding: data transmission over networks (streaming, patches distribution, ...)

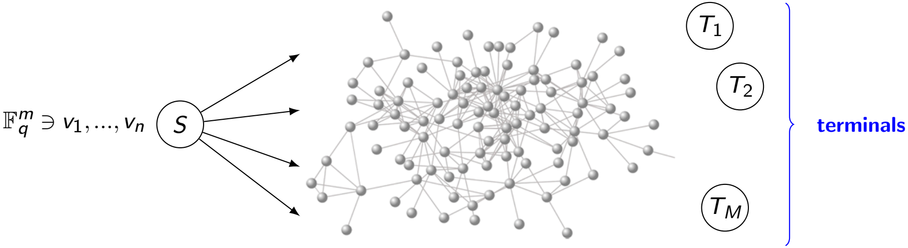


- One source S attempts to transmit messages $v_1, \ldots, v_n \in \mathbb{F}_q^m$.
- The terminals demand **all** the messages (multicast).

What should the nodes do?

What is network coding about?

Network coding: data transmission over networks (streaming, patches distribution, ...)



- One source S attempts to transmit messages $v_1, \dots, v_n \in \mathbb{F}_q^m$.
- The terminals demand **all** the messages (multicast).

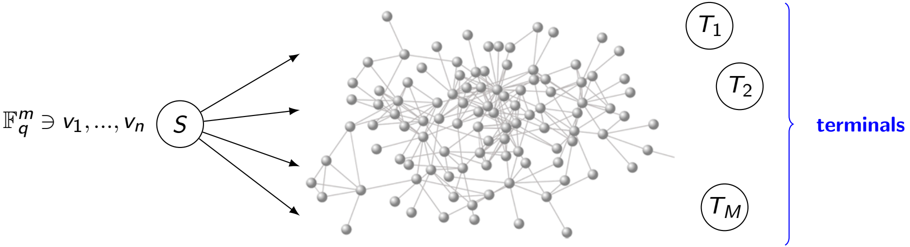
What should the nodes do?

Goal

Maximize the messages that are transmitted to **all** terminals per channel use (**rate**).

What is network coding about?

Network coding: data transmission over networks (streaming, patches distribution, ...)



- One source S attempts to transmit messages $v_1, \dots, v_n \in \mathbb{F}_q^m$.
- The terminals demand **all** the messages (multicast).

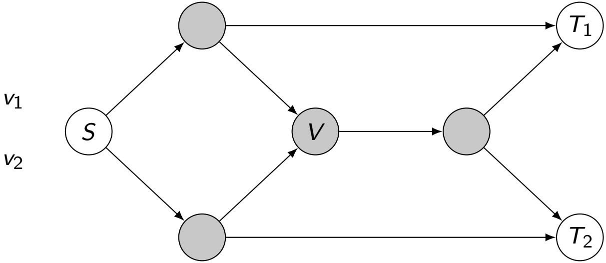
What should the nodes do?

Goal

Maximize the messages that are transmitted to **all** terminals per channel use (**rate**).

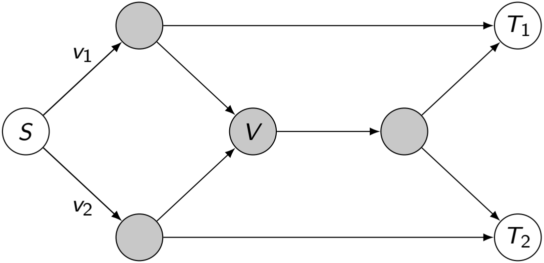
IDEA (Ahlswede-Cai-Li-Yeung 2000): allow the nodes to recombine packets.

The "Butterfly" network

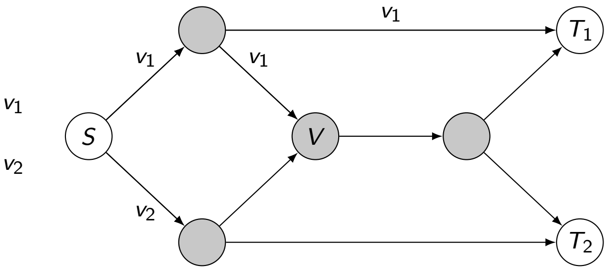


v_1

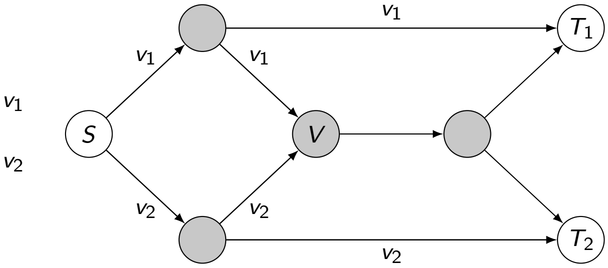
v_2



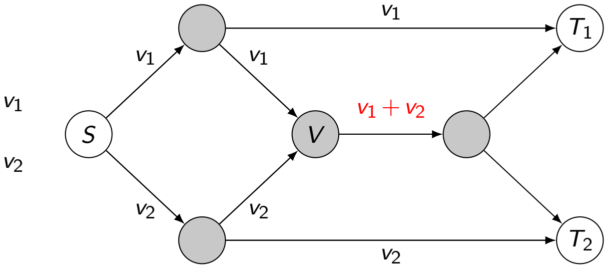
The "Butterfly" network

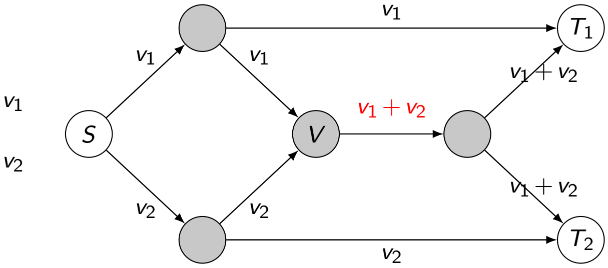


The "Butterfly" network



The "Butterfly" network





This strategy is better than routing.

Networks

Definition

A **(single-source) network** is a 4-tuple $\mathscr{N} = (\mathscr{V}, \mathscr{E}, S, \mathbf{T})$ where:

1. $(\mathscr{V}, \mathscr{E})$ is a finite directed acyclic multigraph,
2. $S \in \mathscr{V}$ is the **source**,
3. $\mathbf{T} \subseteq \mathscr{V}$ is the set of **terminals** or **sinks**.

Definition

A (**single-source**) **network** is a 4-tuple $\mathscr{N} = (\mathscr{V}, \mathscr{E}, S, \mathbf{T})$ where:

1. $(\mathscr{V}, \mathscr{E})$ is a finite directed acyclic multigraph,
2. $S \in \mathscr{V}$ is the **source**,
3. $\mathbf{T} \subseteq \mathscr{V}$ is the set of **terminals** or **sinks**.

(We allow multiple parallel directed edges). We also assume that the following hold.

4. $|\mathbf{T}| \geq 1$, $S \notin \mathbf{T}$.
5. For any $T \in \mathbf{T}$ there exists a directed path from S to T.
6. S does not have incoming edges, and terminals $T \in \mathbf{T}$ do not have outgoing edges.
7. For every vertex $V \in \mathscr{V} \setminus (\{S\} \cup \mathbf{T})$ there exists a directed path from S to V and a directed path from V to T for some $T \in \mathbf{T}$.

Definition

A (**single-source**) **network** is a 4-tuple $\mathscr{N} = (\mathscr{V}, \mathscr{E}, S, \mathbf{T})$ where:

1. $(\mathscr{V}, \mathscr{E})$ is a finite directed acyclic multigraph,
2. $S \in \mathscr{V}$ is the **source**,
3. $\mathbf{T} \subseteq \mathscr{V}$ is the set of **terminals** or **sinks**.

(We allow multiple parallel directed edges). We also assume that the following hold.

4. $|\mathbf{T}| \geq 1$, $S \notin \mathbf{T}$.
5. For any $T \in \mathbf{T}$ there exists a directed path from S to T.
6. S does not have incoming edges, and terminals $T \in \mathbf{T}$ do not have outgoing edges.
7. For every vertex $V \in \mathscr{V} \setminus (\{S\} \cup \mathbf{T})$ there exists a directed path from S to V and a directed path from V to T for some $T \in \mathbf{T}$.

The elements of $\mathscr{V}$ are the **nodes**. The elements of $\mathscr{V} \setminus (\{S\} \cup \mathbf{T})$ are the **intermediate** nodes. We denote the set of incoming and outgoing edges of a $V \in \mathscr{V}$ by $\mathrm{in}(V)$ and $\mathrm{out}(V)$, respectively.

Min-cut bound

- $\mathscr{N}$ the network
- S the source
- $\mathbf{T} = \{T_1, ..., T_M\}$ the set of terminals

Theorem (Ahlswede-Cai-Li-Yeung 2000)

The (multicast) rate of any communication over $\mathscr{N}$ satisfies

$$\text{rate} \leq \mu(\mathscr{N}) := \min\{\text{min-cut}(S, T_i) \mid 1 \leq i \leq M\},$$

where min-cut(S, T_i) is the min. # of edges that one has to remove in $\mathscr{N}$ to disconnect S and T_i.

Min-cut bound

- $\mathscr{N}$ the network
- S the source
- $\mathbf{T} = \{T_1, ..., T_M\}$ the set of terminals

Theorem (Ahlswede-Cai-Li-Yeung 2000)

The (multicast) rate of any communication over $\mathscr{N}$ satisfies

$$\text{rate} \leq \mu(\mathscr{N}) := \min\{\text{min-cut}(S, T_i) \mid 1 \leq i \leq M\},$$

where min-cut(S, T_i) is the min. # of edges that one has to remove in $\mathscr{N}$ to disconnect S and T_i.

Question

Can we design node operations (**network code**) so that the bound is achieved?

Min-cut bound

- $\mathscr{N}$ the network
- S the source
- $\mathbf{T} = \{T_1, \ldots, T_M\}$ the set of terminals

Theorem (Ahlswede-Cai-Li-Yeung 2000)

The (multicast) rate of any communication over $\mathscr{N}$ satisfies

$$\text{rate} \leq \mu(\mathscr{N}) := \min\{\text{min-cut}(S, T_i) \mid 1 \leq i \leq M\},$$

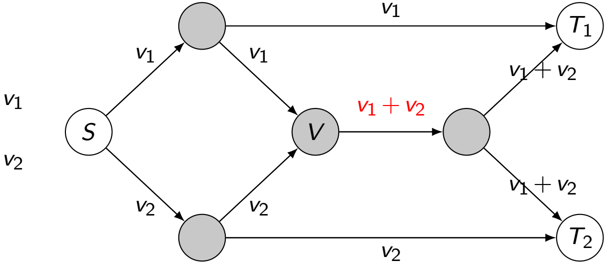
where min-cut(S, T_i) is the min. # of edges that one has to remove in $\mathscr{N}$ to disconnect S and T_i.

Question

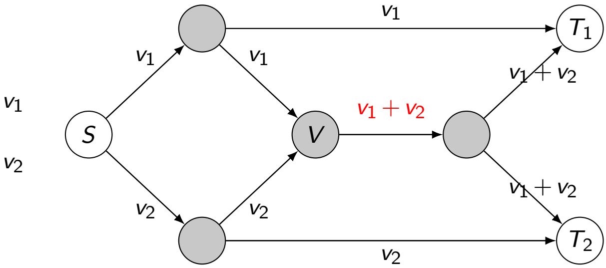
Can we design node operations (**network code**) so that the bound is achieved?

YES, if $q \gg 0$. In fact, **linear operations** suffice.

Example



Example



$$\text{min-cut}(S, T_1) = \text{min-cut}(S, T_2) = 2 \quad \Rightarrow \quad \mu(\mathcal{N}) = 2.$$

Therefore the strategy is optimal over any field $\mathbb{F}_q$.

Moreover, the node operations are linear.

The max-flow-min-cut theorem

(not the max-flow-min-cut theorem from graph theory)

The max-flow-min-cut theorem

(not the max-flow-min-cut theorem from graph theory)

Let $\mathscr{N}$ be a network, and let $\boxed{n = \mu(\mathscr{N})}$. Assume that:

- the source S sends messages $v_1, \dots, v_n \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- terminal T collects $w_1^T, \dots, w_{r(T)}^T$ from the incoming edges, where $r(T) = |\mathrm{in}(T)|$.

The max-flow-min-cut theorem

(not the max-flow-min-cut theorem from graph theory)

Let $\mathscr{N}$ be a network, and let $\boxed{n = \mu(\mathscr{N})}$. Assume that:

- the source S sends messages $v_1, \dots, v_n \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- terminal T collects $w_1^T, \dots, w_{r(T)}^T$ from the incoming edges, where $r(T) = |\mathrm{in}(T)|$.

Then we can write:

$$\begin{bmatrix} w_1^T \\ w_2^T \\ \vdots \\ w_{r(T)}^T \end{bmatrix} = G(T) \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix},$$

where $G(T) \in \mathbb{F}_q^{r(T) \times n}$ is the **transfer matrix** at T, describing all linear nodes operations.

The max-flow-min-cut theorem

(not the max-flow-min-cut theorem from graph theory)

Let $\mathscr{N}$ be a network, and let $\boxed{n = \mu(\mathscr{N})}$. Assume that:

- the source S sends messages $v_1, \ldots, v_n \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- terminal T collects $w_1^T, \ldots, w_{r(T)}^T$ from the incoming edges, where $r(T) = |\mathrm{in}(T)|$.

Then we can write:

$$\begin{bmatrix} w_1^T \\ w_2^T \\ \vdots \\ w_{r(T)}^T \end{bmatrix} = G(T) \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix},$$

where $G(T) \in \mathbb{F}_q^{r(T) \times n}$ is the **transfer matrix** at T, describing all linear nodes operations.

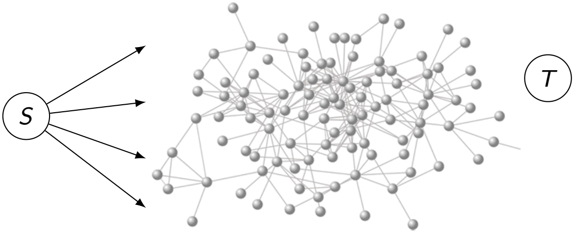
Theorem (Li-Yeung-Cai 2002; Kötter-Médard 2003)

1. Without loss of generality, $r(T) = n = \mu(\mathscr{N})$ for all $T \in \mathbf{T}$.
2. If $q \geq |\mathbf{T}|$, then there exist linear nodes operations such that $G(T)$ is a $n \times n$ invertible matrix for each terminal $T \in \mathbf{T}$, **simultaneously**.

The max-flow-min-cut theorem

Let $n = \mu(\mathcal{N})$.

$$\mathbb{F}_q^{n \times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$



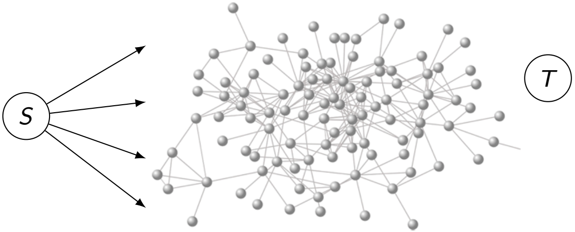
$$G(T) \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

where $G(T) \in \mathbb{F}_q^{n \times n}$ is invertible for every $T \in \mathbf{T}$ $\quad (q \gg 0)$.

The max-flow-min-cut theorem

Let $n = \mu(\mathscr{N})$.

$$\mathbb{F}_q^{n \times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$



$$G(T) \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

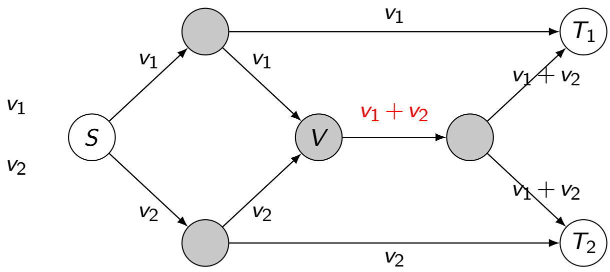
where $G(T) \in \mathbb{F}_q^{n \times n}$ is invertible for every $T \in \mathbf{T}$ $\quad (q \gg 0)$.

Decoding

$$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = G(T)^{-1} \left(G(T) \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \right).$$

Each terminal $T \in \mathbf{T}$ computes the inverse of its own transfer matrix $G(T)$.

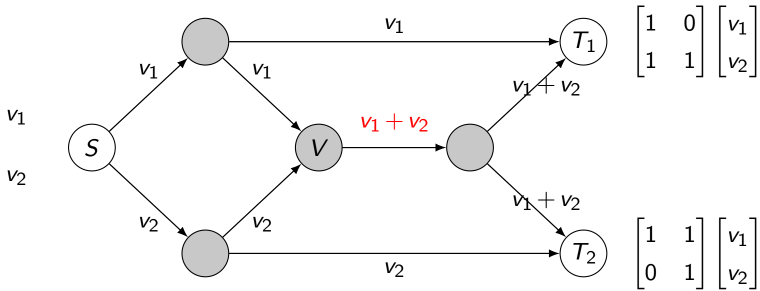
The max-flow-min-cut theorem



$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

The max-flow-min-cut theorem



To summarize:

Theorem

The (multicast) rate of any communication over $\mathscr{N}$ satisfies

$$\text{rate} \leq \mu(\mathscr{N}) := \min\{\text{min-cut}(S, T_i) \mid 1 \leq i \leq M\}.$$

Moreover, if q is sufficiently large the rate is achievable <u>in one shot</u> with <u>linear</u> NC.

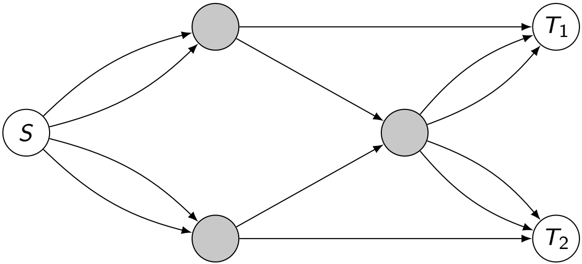
Error correction in networks

The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).

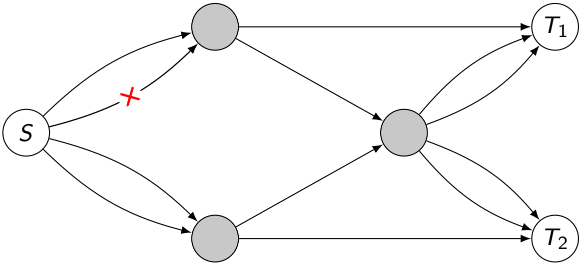
The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



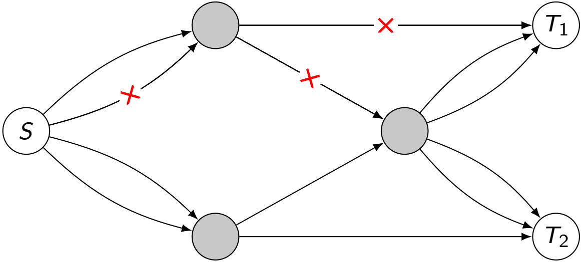
The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



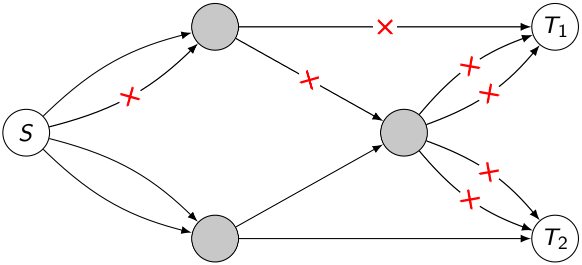
The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



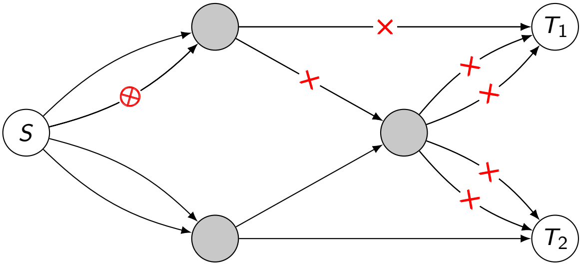
The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



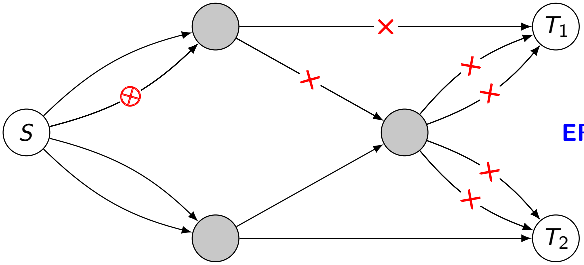
The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



The model

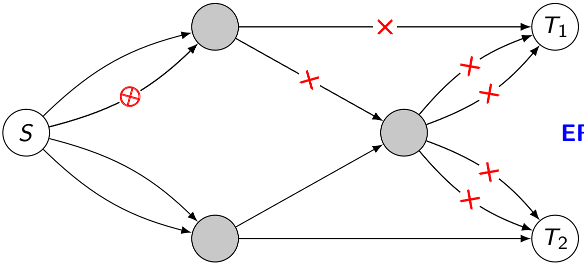
- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).



ERROR AMPLIFICATION

The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).

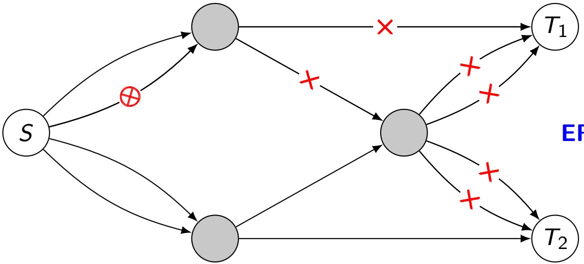


ERROR AMPLIFICATION

Natural solution: design the node operations carefully (decoding at intermediate nodes).

The model

- One adversary can change the value of up to t edges (t is the adversarial *strength*).
- The adversary knows the network code (pre-assigned, linear or not).

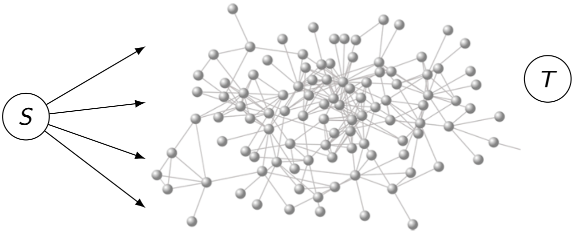


ERROR AMPLIFICATION

Natural solution: design the node operations carefully (decoding at intermediate nodes).
Other solution: use rank-metric codes.

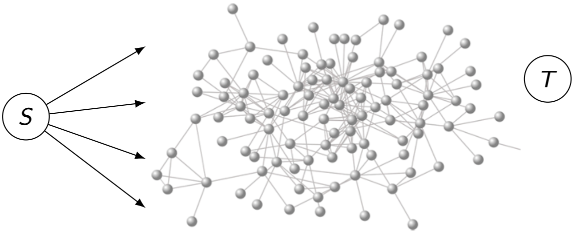
Error correction in networks

Suppose we use linear network coding, $n = \mu(\mathscr{N})$.



Suppose we use linear network coding, $n = \mu(\mathcal{N})$.

$$\mathbb{F}_q^{n\times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = X$$



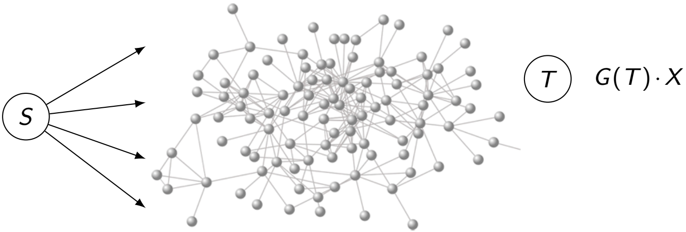
$G(T)\cdot X$

$G(T) \in \mathbb{F}_q^{n\times n}$ is invertible for all $T \in \mathbf{T}$ $\quad (q \gg 0)$.

Error correction in networks

Suppose we use <u>linear</u> network coding, $n = \mu(\mathcal{N})$.

$$\mathbb{F}_q^{n\times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = X$$



$G(T) \in \mathbb{F}_q^{n\times n}$ is invertible for all $T \in \mathbf{T}$ $(q \gg 0)$.

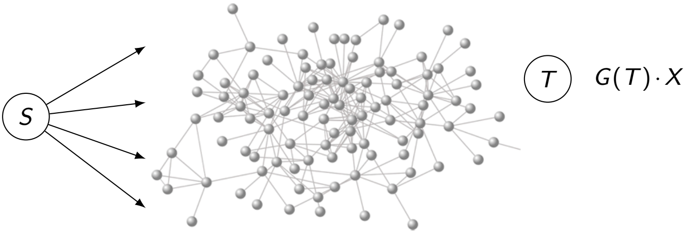
In an error-free context: X is sent, $G(T)\cdot X$ is received by terminal $T \in \mathbf{T}$.

If errors occur: X is sent, $Y(T) \neq G(T)\cdot X$ is received by terminal $T \in \mathbf{T}$.

Error correction in networks

Suppose we use linear network coding, $n = \mu(\mathcal{N})$.

$$\mathbb{F}_q^{n \times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = X$$



$G(T) \in \mathbb{F}_q^{n \times n}$ is invertible for all $T \in \mathbf{T}$ $\quad (q \gg 0)$.

In an error-free context: X is sent, $G(T) \cdot X$ is received by terminal $T \in \mathbf{T}$.

If errors occur: X is sent, $Y(T) \neq G(T) \cdot X$ is received by terminal $T \in \mathbf{T}$.

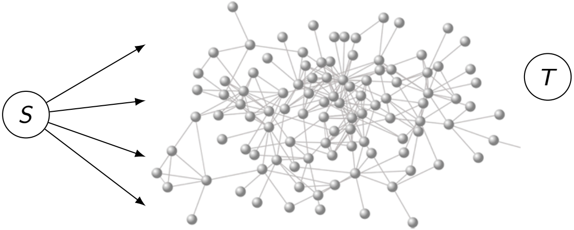
Theorem (Silva-Kschischang-Koetter 2008)

If at most t edges were corrupted, then $\mathrm{rk}(Y(T) - G(T) \cdot X) \leq t$ for all $T \in \mathbf{T}$.

Error correction in networks

Suppose we use linear network coding, $n = \mu(\mathcal{N})$.

$$\mathbb{F}_q^{n\times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = X$$



$G(T) \cdot X$

$G(T) \in \mathbb{F}_q^{n\times n}$ is invertible for all $T \in \mathbf{T}$ $\quad (q \gg 0)$.

In an error-free context: X is sent, $G(T)\cdot X$ is received by terminal $T \in \mathbf{T}$.

If errors occur: X is sent, $Y(T) \neq G(T)\cdot X$ is received by terminal $T \in \mathbf{T}$.

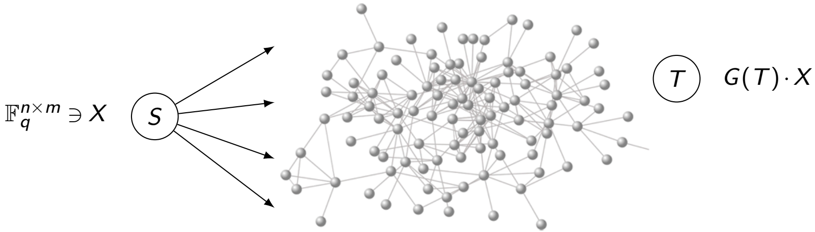
Theorem (Silva-Kschischang-Koetter 2008)

If at most t edges were corrupted, then $\mathrm{rk}(Y(T) - G(T)\cdot X) \leq t$ for all $T \in \mathbf{T}$.

IDEA: use the **rank metric** as a measure of the discrepancy between $Y(T)$ and $G(T)\cdot X$.

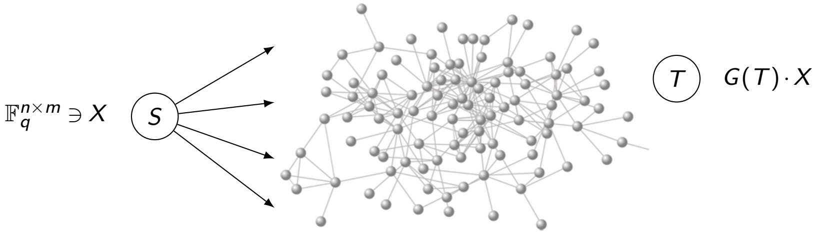
$$d_{\mathrm{rk}}(A,B) = \mathrm{rk}(A-B).$$

Error correction in networks



- What was sent: X
- What should have been received: $G(T) \cdot X$
- What was received: $Y(T)$

Error correction in networks



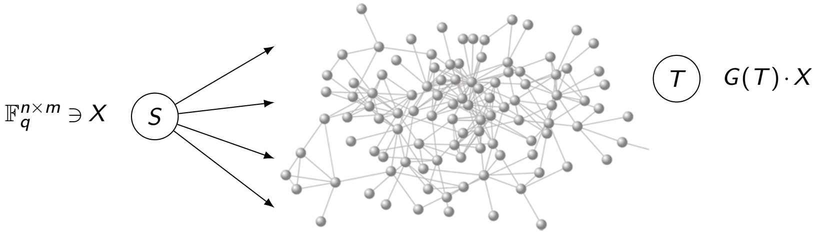
- What was sent: X
- What should have been received: $G(T)\cdot X$
- What was received: $Y(T)$

Theorem (Silva-Kschischang-Koetter 2008)

The adversarial strength t is an upper bound for the rank distance

$$d_{\mathrm{rk}}(Y(T), G(T)\cdot X) \;=\; d_{\mathrm{rk}}(G(T)^{-1}\cdot Y(T), X).$$

Error correction in networks



- What was sent: X
- What should have been received: $G(T)\cdot X$
- What was received: $Y(T)$

Theorem (Silva-Kschischang-Koetter 2008)

The adversarial strength t is an upper bound for the rank distance

$$d_{\mathrm{rk}}(Y(T), G(T)\cdot X) \;=\; d_{\mathrm{rk}}(G(T)^{-1}\cdot Y(T), X).$$

According to this metric, errors propagate but **do not amplify**.

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(X) \mid X \in \mathscr{C},\, X \neq 0\}.$$

Rank-metric codes

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(X) \mid X \in \mathscr{C},\, X \neq 0\}.$$

Communication schemes based on rank-metric codes are:

(1) capacity-achieving (for $q \gg 0$)

(2) compatible with linear network coding

(3) **separable**: network code and rank-metric code can be designed independently

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(X) \mid X \in \mathscr{C},\ X \neq 0\}.$$

Communication schemes based on rank-metric codes are:

(1) capacity-achieving (for $q \gg 0$)

(2) compatible with linear network coding

(3) **separable**: network code and rank-metric code can be designed independently

Theorem (R.-Kschischang)

For more general scenarios, there is no capacity-achieving scheme with (2) and (3).

E.g., multiple adversaries, erasure adversaries, or restricted adversaries.
We study these in *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.

Rank-metric codes

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum distance** is

$$d_{\text{rk}}(\mathscr{C}) = \min\{\text{rk}(X) \mid X \in \mathscr{C},\, X \neq 0\}.$$

Communication schemes based on rank-metric codes are:

(1) capacity-achieving (for $q \gg 0$)

(2) compatible with linear network coding

(3) **separable**: network code and rank-metric code can be designed independently

Theorem (R.-Kschischang)

For more general scenarios, there is no capacity-achieving scheme with (2) and (3).

E.g., multiple adversaries, erasure adversaries, or restricted adversaries.
We study these in *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.

⚠ **ACHTUNG!** Noise is **adversarial**. Probabilistic models require different methods.

Outline

1. Network coding
2. Rank-metric codes and q-polymatroids

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(M) \mid M \in \mathscr{C},\ M \neq 0\}.$$

Rank-metric codes

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(M) \mid M \in \mathscr{C},\ M \neq 0\}.$$

Codes as math objects $\rightsquigarrow$ connections to other areas of mathematics:

- rank-metric codes and association schemes
- rank-metric codes and q-designs
- rank-metric codes and lattices
- rank-metric codes and semifields
- rank-metric codes and q-rook polynomials
- rank-metric codes and q-polymatroids

Rank-metric codes

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-subspace $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$. Its **minimum distance** is

$$d_{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(M) \mid M \in \mathscr{C},\ M \neq 0\}.$$

Codes as math objects $\rightsquigarrow$ connections to other areas of mathematics:

- rank-metric codes and association schemes
- rank-metric codes and q-designs
- rank-metric codes and lattices
- rank-metric codes and semifields
- rank-metric codes and q-rook polynomials
- rank-metric codes and q-polymatroids $\leftarrow$ with E. Gorla, H. López and R. Jurrius

Goal (among others)

Give a combinatorial interpretation to **generalized rank weights**.

Generalized rank weights

For $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$,

$$\mathrm{maxrk}(\mathscr{C}) = \max\{\mathrm{rk}(M) \mid M \in \mathscr{C}\}.$$

Proposition

$\dim(\mathscr{C}) \leq \max\{n, m\} \cdot \mathrm{maxrk}(\mathscr{C})$.

Definition

$\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ is an **optimal anticode** if it meets the bound.

Generalized rank weights

For $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$,
$$\mathrm{maxrk}(\mathscr{C}) = \max\{\mathrm{rk}(M) \mid M \in \mathscr{C}\}.$$

Proposition

$\dim(\mathscr{C}) \leq \max\{n, m\} \cdot \mathrm{maxrk}(\mathscr{C})$.

Definition

$\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ is an **optimal anticode** if it meets the bound.

Anticodes are "tools" to study codes.

Definition (R.)

For $1 \leq r \leq k = \dim(\mathscr{C})$, the r-th **generalized (rank) weight** of $\mathscr{C}$ is

$$d_r(\mathscr{C}) \;=\; \frac{1}{m} \; \min\{\dim(\mathscr{A}) \mid \mathscr{A} \text{ is an optimal anticode, } \dim(\mathscr{C} \cap \mathscr{A}) \geq r\}$$

$$k\text{-dimensional code } \mathscr{C} \leq \mathbb{F}_q^{n \times m} \quad \rightsquigarrow \quad (d_1, d_2, \ldots, d_k) \in \mathbb{N}^k.$$

Applications: secret sharing schemes.

Generalized rank weights

Definition

For $1 \leq r \leq k = \dim(\mathscr{C})$, the r-th **generalized** (**rank**) **weight** of $\mathscr{C}$ is

$$d_r(\mathscr{C}) \; = \; \min\{\dim(\mathscr{A}) \mid \mathscr{A} \text{ is an optimal anticode, } \dim(\mathscr{C} \cap \mathscr{A}) \geq r\}$$

Generalized weights are a code invariant.

Definition

For $1 \leq r \leq k = \dim(\mathscr{C})$, the r-th **generalized (rank) weight** of $\mathscr{C}$ is

$$d_r(\mathscr{C}) \;=\; \min\{\dim(\mathscr{A}) \mid \mathscr{A} \text{ is an optimal anticode, } \dim(\mathscr{C} \cap \mathscr{A}) \geq r\}$$

Generalized weights are a code invariant.

Definition

Codes $\mathscr{C}, \mathscr{C}' \leq \mathbb{F}_q^{n \times m}$ are **equivalent** if there exists $f : (\mathbb{F}_q^{n \times m}, d_{\mathrm{rk}}) \to (\mathbb{F}_q^{n \times m}, d_{\mathrm{rk}})$ $\mathbb{F}_q$-linear isometry such that

$$f(\mathscr{C}) = \mathscr{C}'.$$

Remark

Equivalent codes have the same generalized weights.

Definition (Gorla-López-Jurrius-R. 2018)

A q-**polymatroid** is a pair $P = (\mathbb{F}_q^n, \rho)$ where $n \geq 1$ and ρ is a function from the set of subspaces of $\mathbb{F}_q^n$ to $\mathbb{R}$ such that, for all $U, V \leq \mathbb{F}_q^n$:

- $0 \leq \rho(U) \leq \dim(U)$,
- if $U \subseteq V$, then $\rho(U) \leq \rho(V)$,
- $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

Remark: we allow $\rho(U) \notin \mathbb{Z}$.

Definition (Gorla-López-Jurrius-R. 2018)

A q-**polymatroid** is a pair $P = (\mathbb{F}_q^n, \rho)$ where $n \geq 1$ and ρ is a function from the set of subspaces of $\mathbb{F}_q^n$ to $\mathbb{R}$ such that, for all $U, V \leq \mathbb{F}_q^n$:

- $0 \leq \rho(U) \leq \dim(U)$,
- if $U \subseteq V$, then $\rho(U) \leq \rho(V)$,
- $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

Remark: we allow $\rho(U) \notin \mathbb{Z}$.

Let $U^\perp$ denote the orthogonal of $U \leq \mathbb{F}_q^n$ w.r. to the standard inner product.

Theorem (Gorla-López-Jurrius-R. 2018)

Let $P = (\mathbb{F}_q^n, \rho)$ be a q-polymatroid. Define

$$\rho^*(U) = \dim(U) - \rho(\mathbb{F}_q^n) + \rho(U^\perp) \qquad \text{for } U \leq \mathbb{F}_q^n.$$

Then $(\mathbb{F}_q^n, \rho^*)$ is a q-polymatroid. We call it the **dual** of $(\mathbb{F}_q^n, \rho)$.

Codes and q-polymatroids

Let $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ be a rank-metric code. For $U \leq \mathbb{F}_q^n$ and $V \leq \mathbb{F}_q^m$, define the subcodes

$$\begin{aligned} \mathscr{C}^{\mathrm{cs}}(U) &= \{X \in \mathscr{C} \mid \mathrm{cs}(X) \leq U\} \leq \mathscr{C}, \\ \mathscr{C}^{\mathrm{rs}}(V) &= \{X \in \mathscr{C} \mid \mathrm{rs}(X) \leq V\} \leq \mathscr{C}. \end{aligned}$$

Codes and q-polymatroids

Let $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ be a rank-metric code. For $U \leq \mathbb{F}_q^n$ and $V \leq \mathbb{F}_q^m$, define the subcodes

$$\begin{aligned} \mathscr{C}^{\mathrm{cs}}(U) &= \{X \in \mathscr{C} \mid \mathrm{cs}(X) \leq U\} \leq \mathscr{C}, \\ \mathscr{C}^{\mathrm{rs}}(V) &= \{X \in \mathscr{C} \mid \mathrm{rs}(X) \leq V\} \leq \mathscr{C}. \end{aligned}$$

Then let

$$\begin{aligned} \rho_{\mathscr{C}}^{\mathrm{cs}}(U) &= \frac{1}{m}\left(\dim \mathscr{C} - \dim \mathscr{C}^{\mathrm{cs}}(U^\perp)\right), \\ \rho_{\mathscr{C}}^{\mathrm{rs}}(V) &= \frac{1}{m}\left(\dim \mathscr{C} - \dim \mathscr{C}^{\mathrm{rs}}(V^\perp)\right). \end{aligned}$$

Let $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ be a rank-metric code. For $U \leq \mathbb{F}_q^n$ and $V \leq \mathbb{F}_q^m$, define the subcodes

$$\begin{aligned} \mathscr{C}^{\mathrm{cs}}(U) &= \{X \in \mathscr{C} \mid \mathrm{cs}(X) \leq U\} \leq \mathscr{C}, \\ \mathscr{C}^{\mathrm{rs}}(V) &= \{X \in \mathscr{C} \mid \mathrm{rs}(X) \leq V\} \leq \mathscr{C}. \end{aligned}$$

Then let

$$\begin{aligned} \rho_{\mathscr{C}}^{\mathrm{cs}}(U) &= \frac{1}{m}\left(\dim \mathscr{C} - \dim \mathscr{C}^{\mathrm{cs}}(U^\perp)\right), \\ \rho_{\mathscr{C}}^{\mathrm{rs}}(V) &= \frac{1}{m}\left(\dim \mathscr{C} - \dim \mathscr{C}^{\mathrm{rs}}(V^\perp)\right). \end{aligned}$$

Theorem (Gorla-López-Jurrius-R. 2018)

$(\mathbb{F}_q^n, \rho_{\mathscr{C}}^{\mathrm{cs}})$ and $(\mathbb{F}_q^m, \rho_{\mathscr{C}}^{\mathrm{rs}})$ are q-polymatroids.

We associate to a code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ a pair of q-polymatroids.

What do these remember?

$\mathscr{C} \leq \mathbb{F}_q^{n\times m} \rightsquigarrow (\mathbb{F}_q^n, \rho_{\mathscr{C}}^{\mathrm{cs}}),\ (\mathbb{F}_q^m, \rho_{\mathscr{C}}^{\mathrm{rs}})$ **What do these remember?**

- the dimension of $\mathscr{C}$

Proposition (Gorla-López-Jurrius-R. 2018)

$$\begin{aligned} \dim \mathscr{C} &= m \cdot \rho_{\mathscr{C}}^{\mathrm{cs}}(\mathbb{F}_q^n) \\ &= n \cdot \rho_{\mathscr{C}}^{\mathrm{rs}}(\mathbb{F}_q^m) \end{aligned}$$

$\mathscr{C} \le \mathbb{F}_q^{n\times m} \rightsquigarrow (\mathbb{F}_q^n, \rho_{\mathscr{C}}^{\mathrm{cs}}),\ (\mathbb{F}_q^m, \rho_{\mathscr{C}}^{\mathrm{rs}})$ **What do these remember?**

- the dimension of $\mathscr{C}$

Proposition (Gorla-López-Jurrius-R. 2018)

$$\begin{aligned}\dim \mathscr{C} &= m \cdot \rho_{\mathscr{C}}^{\mathrm{cs}}(\mathbb{F}_q^n) \\ &= n \cdot \rho_{\mathscr{C}}^{\mathrm{rs}}(\mathbb{F}_q^m)\end{aligned}$$

- the minimum distance of $\mathscr{C}$

Theorem (Gorla-López-Jurrius-R. 2018)

$$\begin{aligned}d_{\mathrm{rk}}(\mathscr{C}) &= n+1-\min\left\{d \mid \rho_{\mathscr{C}}^{\mathrm{cs}}(U) = \frac{\dim \mathscr{C}}{m} \text{ for all } U \le \mathbb{F}_q^n \text{ with } \dim U = d\right\} \\ &= m+1-\min\left\{d \mid \rho_{\mathscr{C}}^{\mathrm{rs}}(V) = \frac{\dim \mathscr{C}}{n} \text{ for all } V \le \mathbb{F}_q^m \text{ with } \dim V = d\right\}\end{aligned}$$

$\mathscr{C} \leq \mathbb{F}_q^{n\times m} \rightsquigarrow (\mathbb{F}_q^n, \rho_{\mathscr{C}}^{\mathrm{cs}}),\ (\mathbb{F}_q^m, \rho_{\mathscr{C}}^{\mathrm{rs}})$ **What do these remember?**

- the generalized weights of $\mathscr{C}$

Theorem (Gorla-López-Jurrius-R. 2018)

– If $m > n$ we have

$$d_r(\mathscr{C}) = \min\{n - \dim(U) \mid U \leq \mathbb{F}_q^n,\ \dim \mathscr{C} - m\rho_{\mathscr{C}}^{\mathrm{cs}}(U) \geq r\}$$

– If $m < n$ we have

$$d_r(\mathscr{C}) = \min\{m - \dim(V) \mid V \leq \mathbb{F}_q^m,\ \dim \mathscr{C} - n\rho_{\mathscr{C}}^{\mathrm{rs}}(V) \geq r\}$$

– If $n = m$ we have

$$d_r(\mathscr{C}) = \min\{d_r^{\mathrm{cs}}(\mathscr{C}),\ d_r^{\mathrm{rs}}(\mathscr{C})\}$$

where

$$\begin{aligned} d_r^{\mathrm{cs}}(\mathscr{C}) &= \min\{n - \dim(U) \mid U \leq \mathbb{F}_q^n,\ \dim \mathscr{C} - m\rho_{\mathscr{C}}^{\mathrm{cs}}(U) \geq r\} \\ d_r^{\mathrm{rs}}(\mathscr{C}) &= \min\{m - \dim(V) \mid V \leq \mathbb{F}_q^m,\ \dim \mathscr{C} - n\rho_{\mathscr{C}}^{\mathrm{rs}}(V) \geq r\} \end{aligned}$$

Other connections between codes and q-polymatroids:

Theorem (Gorla-López-Jurrius-R. 2018)

- The property of being an optimal (MRD) code is captured by the q-polymatroids
- The property of being an optimal anticode code is captured by the q-polymatroids
- The q-polymatroids of $\mathscr{C}^\perp$ are the duals of the q-polymatoids of $\mathscr{C}$
- Equivalent codes have equivalent q-polymatroids

Other connections between codes and q-polymatroids:

Theorem (Gorla-López-Jurrius-R. 2018)

- The property of being an optimal (MRD) code is captured by the q-polymatroids
- The property of being an optimal anticode code is captured by the q-polymatroids
- The q-polymatroids of $\mathscr{C}^\perp$ are the duals of the q-polymatoids of $\mathscr{C}$
- Equivalent codes have equivalent q-polymatroids

Thank you very much!