Network Coding, Rank-Metric Codes, and Rook Theory

Alberto Ravagnani

University College Dublin

Miniconference "c_2 Invariant Meets Rook Theory"

Berlin, Apr. 2019

Outline

1. Network coding
2. Rank-metric codes and topics in combinatorics

Outline

1. Network coding

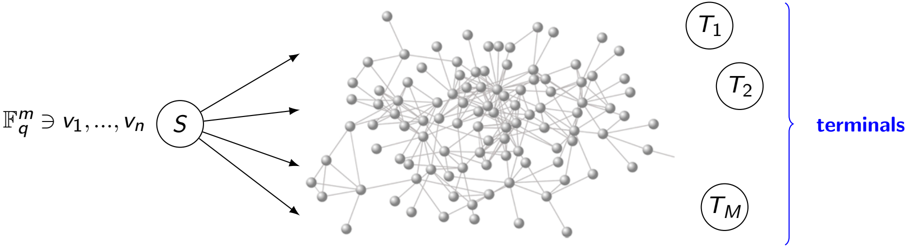
2. Rank-metric codes and topics in combinatorics

What is network coding about?

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

What is network coding about?

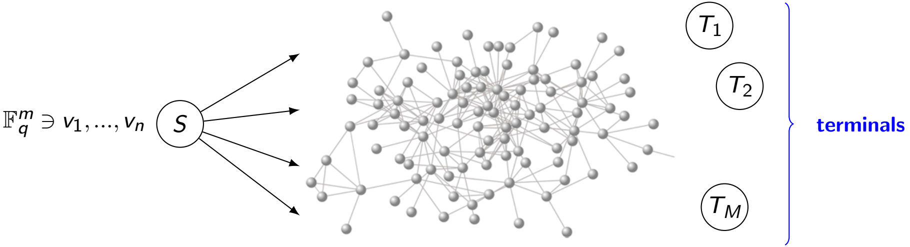
Network coding: data transmission over networks (streaming, patches distribution, ...)



- 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 is network coding about?

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

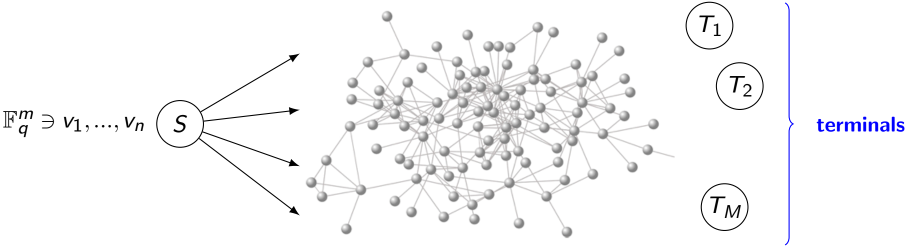


- One source S attempts to transmit messages $v_1, \dots, v_n \in \mathbb{F}_q^m$.
- The terminals demand **all** the messages (multicast).

What should the nodes do?

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).

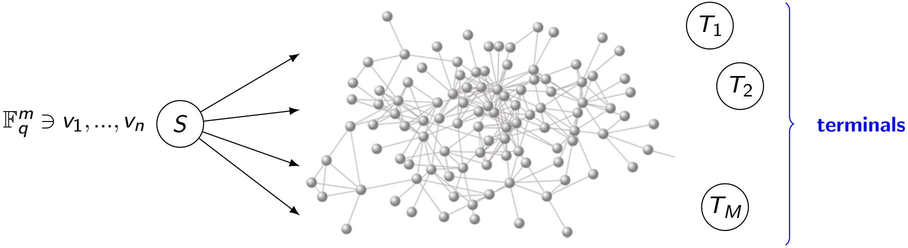
What should the nodes do?

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

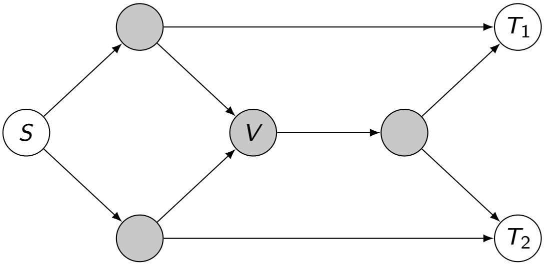
Maximize the messages that are transmitted to **all** terminals per channel use (**rate**).

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

The "Butterfly" network

v_1

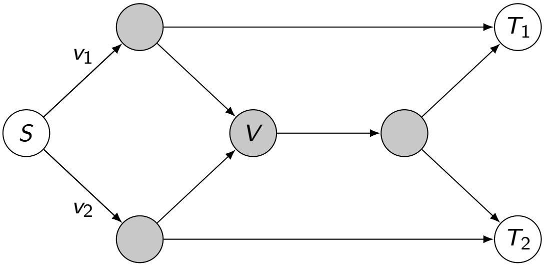
v_2



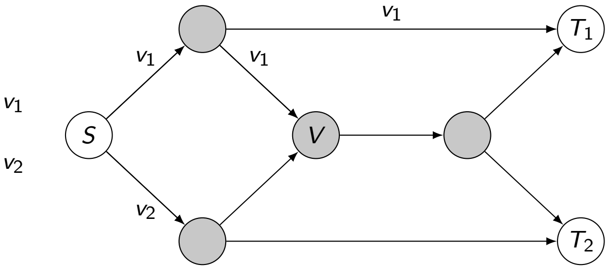
The "Butterfly" network

v_1

v_2



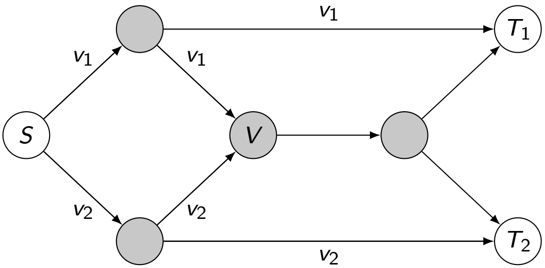
The "Butterfly" network



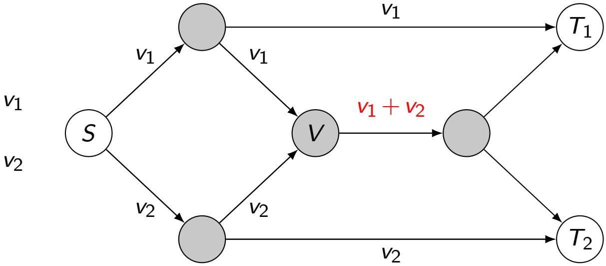
The "Butterfly" network

v_1

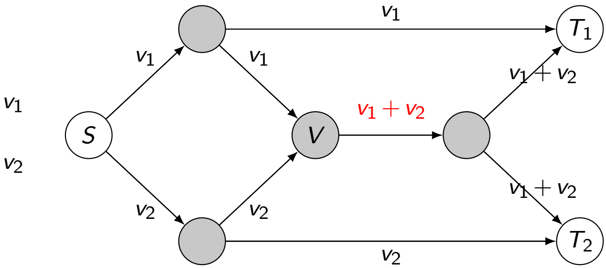
v_2



The "Butterfly" network



The “Butterfly” network



This strategy is better than routing.

Min-cut bound

- $\mathcal{N}$ 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 $\mathcal{N}$ satisfies

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

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

Min-cut bound

- $\mathcal{N}$ 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 $\mathcal{N}$ satisfies

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

where min-cut(S, T_i) is the min. $\#$ of edges that one has to remove in $\mathcal{N}$ 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
- $\mathbf{T} = \{T_1, ..., T_M\}$ the set of terminals

Theorem (Ahlswede-Cai-Li-Yeung 2000)

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

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

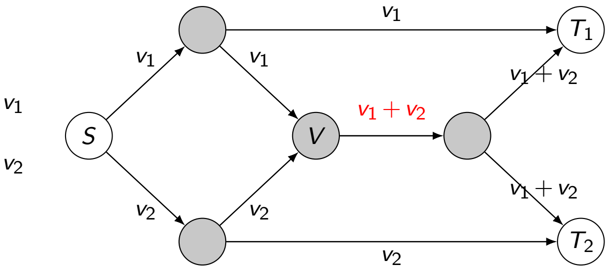
where min-cut(S, T_i) is the min. # of edges that one has to remove in $\mathscr{N}$ to disconnect S and T_i.

Question

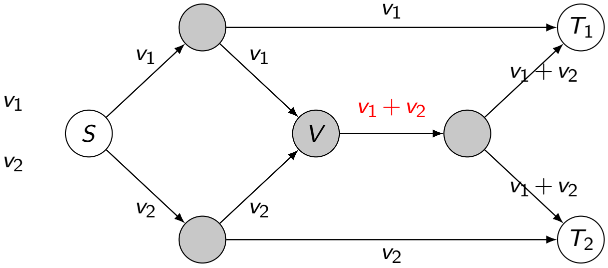
Can we design node operations (**network code**) so that the bound is achieved?

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 $v_1, \ldots, v_n \in \mathbb{F}_q^n$,
- 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.

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.

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 $\mathcal{N}$ be a network, and let $\boxed{n = \mu(\mathcal{N})}$. 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.

Then we can write:

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

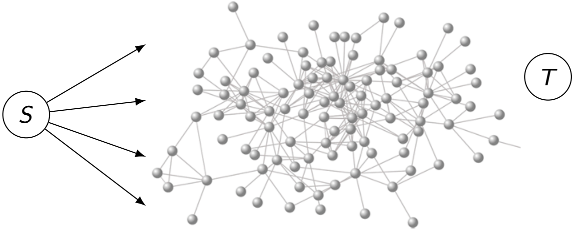
where $G(T) \in \mathbb{F}_q^{r(T) \times n}$ is the **transfer matrix** at T, describing all linear nodes operations.

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

1. Without loss of generality, $r(T) = n = \mu(\mathcal{N})$ 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**.

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

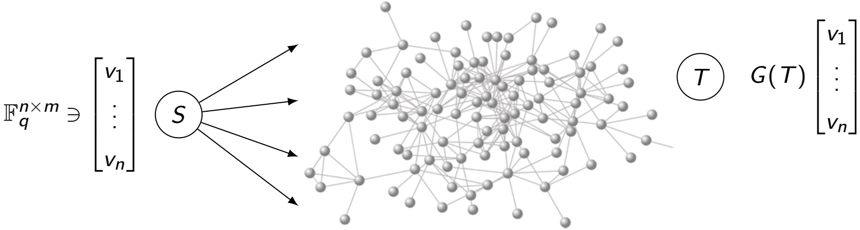
$\mathbb{F}_q^{n \times m} \ni \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$



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

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

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



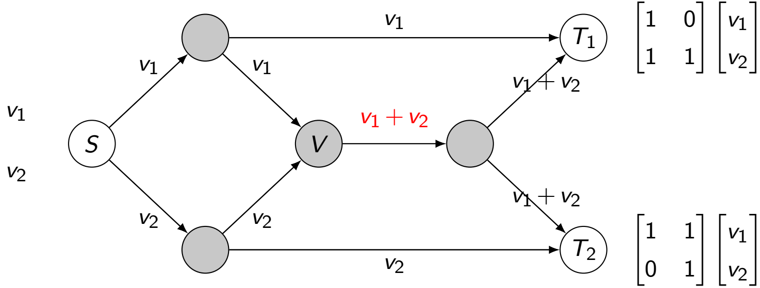
where $G(T) \in \mathbb{F}_q^{n\times n}$ is invertible for every $T \in \mathbf{T}$ $\quad (q \gg 0)$.

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



Error correction in networks

The model

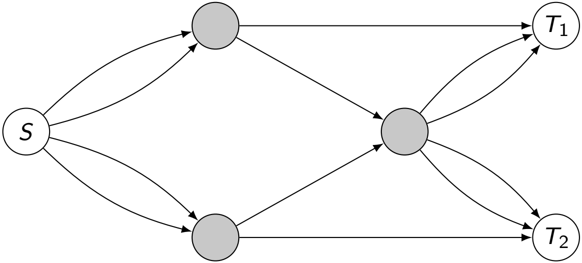
One adversary can change the value of up to t edges (t is the adversarial *strength*).

Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.

The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

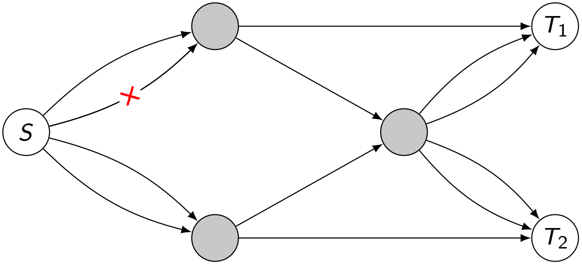
Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

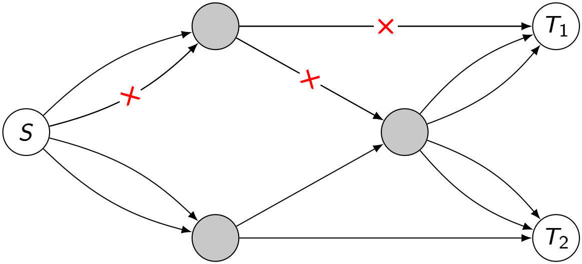
Other models are possible (restricted avdersaries, erasures, ...). We study these in:
Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

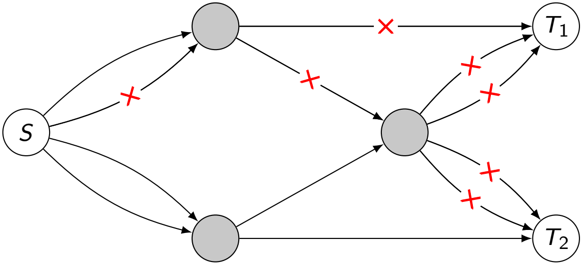
Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

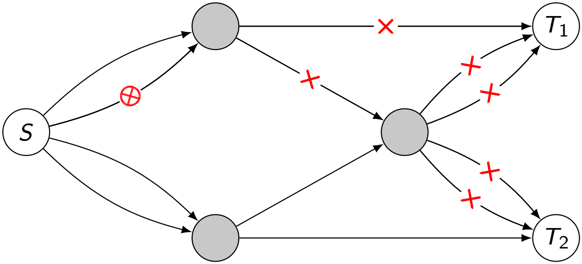
Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

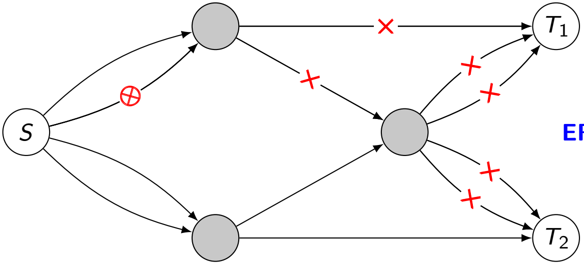
Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.

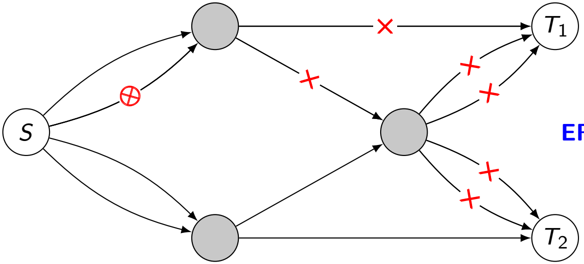


ERROR AMPLIFICATION

The model

One adversary can change the value of up to t edges (t is the adversarial *strength*).

Other models are possible (restricted avdersaries, erasures, ...). We study these in:
Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.



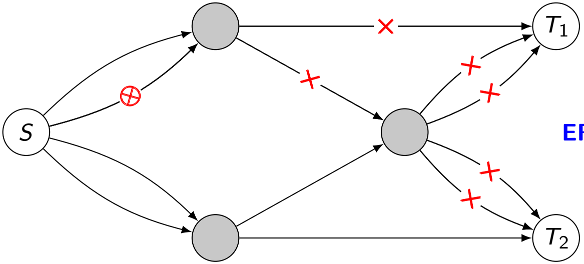
ERROR AMPLIFICATION

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*).

Other models are possible (restricted avdersaries, erasures, ...). We study these in: Kschischang, R., *Adversarial Network Coding*, IEEE Trans. Inf. Th. 2018.

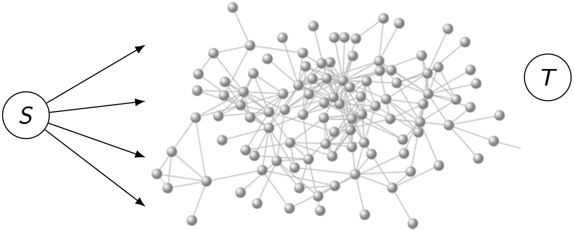


ERROR AMPLIFICATION

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

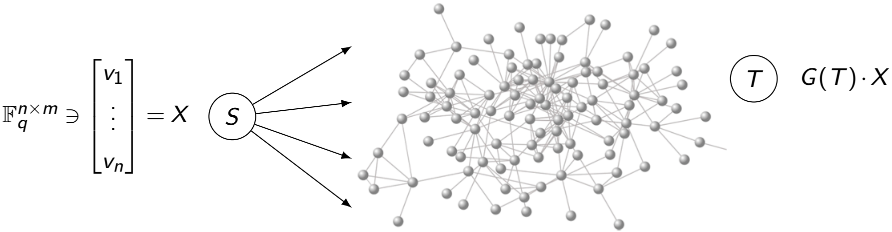
Error correction in networks

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



Error correction in networks

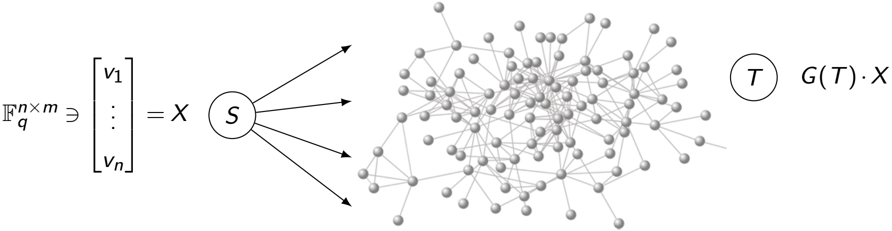
Suppose we use linear network coding, $n = \mu(\mathcal{N})$.



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

Error correction in networks

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



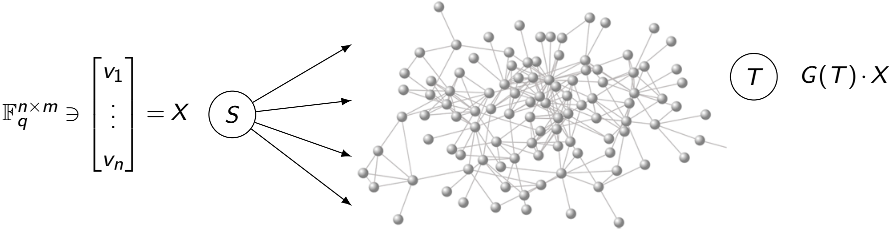
$G(T) \in \mathbb{F}_q^{n \times n}$ is invertible for all $T \in \mathbf{T}$ $\quad (q \gg 0)$.

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 $T \in \mathbf{T}$.

Error correction in networks

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



$G(T) \in \mathbb{F}_q^{n\times n}$ 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 $T \in \mathbf{T}$.

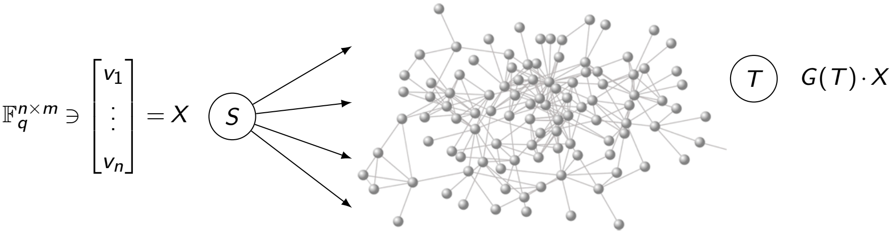
If errors occur: X is sent, $Y(T) \neq G(T)\cdot X$ is received by terminal $T \in \mathbf{T}$.

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



$G(T) \in \mathbb{F}_q^{n\times n}$ 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 $G(T)\cdot X$.

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

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 (also called subspace designs)
- rank-metric codes and lattices
- rank-metric codes and semifields
- rank-metric codes and q-rook polynomials
- rank-metric codes and q-polymatroids

(In the sequel, we assume $m \geq n$ w.l.o.g.)

Outline

1. Network coding
2. Rank-metric codes and topics in combinatorics

MacWilliams identities for the rank metric

Notion of duality in $\mathbb{F}_q^{n\times m}$: the **trace-product** of $M,N\in\mathbb{F}_q^{n\times m}$ is $\langle M,N\rangle := \mathrm{Tr}(MN^\top)$.

Definition

The **dual** of a rank-metric code $\mathscr{C}\le\mathbb{F}_q^{n\times m}$ is

$$\mathscr{C}^\perp := \{N\in\mathbb{F}_q^{n\times m} \mid \langle M,N\rangle = 0 \text{ for all } M\in\mathscr{C}\}.$$

MacWilliams identities for the rank metric

Notion of duality in $\mathbb{F}_q^{n\times m}$: the **trace-product** of $M,N \in \mathbb{F}_q^{n\times m}$ is $\langle M,N\rangle := \mathrm{Tr}(MN^\top)$.

Definition

The **dual** of a rank-metric code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ is

$$\mathscr{C}^\perp := \{N \in \mathbb{F}_q^{n\times m} \mid \langle M,N\rangle = 0 \text{ for all } M \in \mathscr{C}\}.$$

We count the number of rank i matrices in a rank-metric code:

$$W_i(\mathscr{C}) := |\{M \in \mathscr{C} \mid \mathrm{rk}(M) = i\}| \qquad \textbf{(rank enumerator)}$$

MacWilliams identities for the rank metric

Notion of duality in $\mathbb{F}_q^{n\times m}$: the **trace-product** of $M,N \in \mathbb{F}_q^{n\times m}$ is $\langle M,N\rangle := \mathrm{Tr}(MN^\top)$.

Definition

The **dual** of a rank-metric code $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ is

$$\mathscr{C}^\perp := \{N \in \mathbb{F}_q^{n\times m} \mid \langle M,N\rangle = 0 \text{ for all } M \in \mathscr{C}\}.$$

We count the number of rank i matrices in a rank-metric code:

$$W_i(\mathscr{C}) := |\{M \in \mathscr{C} \mid \mathrm{rk}(M) = i\}| \qquad \textbf{(rank enumerator)}$$

Theorem (Delsarte)

Let $\mathscr{C} \le \mathbb{F}_q^{n\times m}$, and let $0 \le j \le n$. we have

$$W_j(\mathscr{C}^\perp) = \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} W_i(\mathscr{C}) \sum_{s=0}^{n} (-1)^{j-s} \, q^{ms+\binom{j-s}{2}} \begin{bmatrix} n-i \\ s \end{bmatrix}_q \begin{bmatrix} n-s \\ j-s \end{bmatrix}_q .$$

Original proof by Delsarte uses association schemes and recurrence relations.

MacWilliams identities for the rank metric

For a code $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ and a subspace $U \leq \mathbb{F}_q^n$, let

$$\begin{aligned} f_{\mathscr{C}}(U) &:= |\{M \in \mathscr{C} \mid \text{col-space}(M) = U\}| \\ g_{\mathscr{C}}(U) &:= \sum_{V \leq U} f_{\mathscr{C}}(V) \;=\; |\{M \in \mathscr{C} \mid \text{col-space}(M) \subseteq U\}| \end{aligned}$$

MacWilliams identities for the rank metric

For a code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ and a subspace $U \leq \mathbb{F}_q^n$, let

$$
\begin{aligned}
f_{\mathscr{C}}(U) &:= |\{M \in \mathscr{C} \mid \text{col-space}(M) = U\}| \\
g_{\mathscr{C}}(U) &:= \sum_{V \leq U} f_{\mathscr{C}}(V) = |\{M \in \mathscr{C} \mid \text{col-space}(M) \subseteq U\}|
\end{aligned}
$$

Note that:

$$
W_j(\mathscr{C}^\perp) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} f_{\mathscr{C}^\perp}(U) =
$$

MacWilliams identities for the rank metric

For a code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ and a subspace $U \leq \mathbb{F}_q^n$, let

$$\begin{aligned} f_{\mathscr{C}}(U) &:= |\{M \in \mathscr{C} \mid \text{col-space}(M) = U\}| \\ g_{\mathscr{C}}(U) &:= \sum_{V \leq U} f_{\mathscr{C}}(V) = |\{M \in \mathscr{C} \mid \text{col-space}(M) \subseteq U\}| \end{aligned}$$

Note that:

$$W_j(\mathscr{C}^\perp) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} f_{\mathscr{C}^\perp}(U) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}}$$

MacWilliams identities for the rank metric

For a code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ and a subspace $U \leq \mathbb{F}_q^n$, let

$$\begin{aligned} f_{\mathscr{C}}(U) &:= |\{M \in \mathscr{C} \mid \text{col-space}(M) = U\}| \\ g_{\mathscr{C}}(U) &:= \sum_{V \leq U} f_{\mathscr{C}}(V) = |\{M \in \mathscr{C} \mid \text{col-space}(M) \subseteq U\}| \end{aligned}$$

Note that:

$$W_j(\mathscr{C}^\perp) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} f_{\mathscr{C}^\perp}(U) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} \sum_{V \leq U} g_{\mathscr{C}^\perp}(V)\mu(V,U),$$

where μ is the Mœbius function of the lattice of subspaces of $\mathbb{F}_q^n$.

MacWilliams identities for the rank metric

For a code $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ and a subspace $U \leq \mathbb{F}_q^n$, let

$$f_{\mathscr{C}}(U) := |\{M \in \mathscr{C} \mid \text{col-space}(M) = U\}|$$

$$g_{\mathscr{C}}(U) := \sum_{V \leq U} f_{\mathscr{C}}(V) = |\{M \in \mathscr{C} \mid \text{col-space}(M) \subseteq U\}|$$

Note that:

$$W_j(\mathscr{C}^\perp) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} f_{\mathscr{C}^\perp}(U) = \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} \sum_{V \leq U} g_{\mathscr{C}^\perp}(V)\,\mu(V,U),$$

where μ is the Mœbius function of the lattice of subspaces of $\mathbb{F}_q^n$.

Proposition (R.)

$$g_{\mathscr{C}^\perp}(V) = \frac{q^{m \cdot \dim(V)}}{|\mathscr{C}|}\, g_{\mathscr{C}}(V^\perp),$$

where $V^\perp$ is the orthogonal of $V \leq \mathbb{F}_q^n$ w. r. to the standard inner product of $\mathbb{F}_q^n$.

MacWilliams identities for the rank metric

$$W_j(\mathscr{C}^\perp) \quad = \quad \frac{1}{|\mathscr{C}|}\sum_{i=0}^{j}(-1)^{j-i}q^{mi+\binom{j-i}{2}} \sum_{\substack{U\le\mathbb{F}_q^n \\ \dim(U)=j}} \sum_{\substack{V\le U \\ \dim(V)=i}} g_{\mathscr{C}}(V^\perp)$$

MacWilliams identities for the rank metric

$$W_j(\mathscr{C}^\perp) = \frac{1}{|\mathscr{C}|} \sum_{i=0}^{j} (-1)^{j-i} q^{mi+\binom{j-i}{2}} \sum_{\substack{U \leq \mathbb{F}_q^n \\ \dim(U)=j}} \sum_{\substack{V \leq U \\ \dim(V)=i}} g_{\mathscr{C}}(V^\perp)$$

$$\vdots$$

Theorem (Delsarte)

$$W_j(\mathscr{C}^\perp) = \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} W_i(\mathscr{C}) \sum_{s=0}^{n} (-1)^{j-s} \; q^{ms+\binom{j-s}{2}} \begin{bmatrix} n-i \\ s \end{bmatrix}_q \begin{bmatrix} n-s \\ j-s \end{bmatrix}_q$$

Why a new proof?

- nice to see things from a different perspective,
- proof technique can be "exported" to other contexts (**pivot enumerators**).

But before looking at other types of MacWilliams identities...

MacWilliams identities for the rank metric

Why a new proof?

- nice to see things from a different perspective,
- proof technique can be "exported" to other contexts (**pivot enumerators**).

But before looking at other types of MacWilliams identities...

PROBLEMS

Compute the number of rank r matrices $M \in \mathbb{F}_q^{n \times m}$ such that:

- their entries sum to zero,
- a certain set of diagonal entries are zero ($M_{ii} = 0$ for all $i \in I \subseteq \{1, \ldots, n\}$),
- ...

Theorem (R.)

Let $\emptyset \neq I \subseteq \{1,\dots,n\}$. The number of rank r matrices $M \in \mathbb{F}_q^{n \times m}$ with $M_{ii} = 0$ for all $i \in I$ is given by the formula

$$v_r(I) \;:=\; q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^{n} (-1)^{r-s} q^{ms+\binom{r-s}{2}} \begin{bmatrix} n-s \\ n-r \end{bmatrix}_q \begin{bmatrix} n-i \\ s \end{bmatrix}_q .$$

MacWilliams identities for the rank metric

Theorem (R.)

Let $\emptyset \neq I \subseteq \{1,\dots,n\}$. The number of rank r matrices $M \in \mathbb{F}_q^{n\times m}$ with $M_{ii}=0$ for all $i \in I$ is given by the formula

$$v_r(I) \;:=\; q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^{n} (-1)^{r-s} q^{ms+\binom{r-s}{2}} \begin{bmatrix} n-s \\ n-r \end{bmatrix}_q \begin{bmatrix} n-i \\ s \end{bmatrix}_q .$$

Let $\mathscr{C}[I]$ be the space of matrices supported on $\{(i,i) \mid i \in I\}$.

Then $\mathscr{C}[I] \leq \mathbb{F}_q^{n\times m}$ is a linear rank-metric code, and

$$v_r(I) = W_r(\mathscr{C}[I]^\perp)$$

Theorem (R.)

Let $\emptyset \neq I \subseteq \{1,\dots,n\}$. The number of rank r matrices $M \in \mathbb{F}_q^{n\times m}$ with $M_{ii}=0$ for all $i \in I$ is given by the formula

$$v_r(I) \;:=\; q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^{n} (-1)^{r-s} q^{ms+\binom{r-s}{2}} \begin{bmatrix} n-s \\ n-r \end{bmatrix}_q \begin{bmatrix} n-i \\ s \end{bmatrix}_q .$$

Let $\mathscr{C}[I]$ be the space of matrices supported on $\{(i,i) \mid i \in I\}$.

Then $\mathscr{C}[I] \leq \mathbb{F}_q^{n\times m}$ is a linear rank-metric code, and

$$v_r(I) = W_r(\mathscr{C}[I]^\perp) \;=\; \frac{1}{|\mathscr{C}[I]|} \sum_{i=0}^{n} W_i(\mathscr{C}[I]) \sum_{s=0}^{n} (-1)^{j-s}\, q^{ms+\binom{j-s}{2}} \begin{bmatrix} n-i \\ s \end{bmatrix}_q \begin{bmatrix} n-s \\ j-s \end{bmatrix}_q .$$

MacWilliams identities for the rank metric

Theorem (R.)

Let $\emptyset \neq I \subseteq \{1, \dots, n\}$. The number of rank r matrices $M \in \mathbb{F}_q^{n \times m}$ with $M_{ii} = 0$ for all $i \in I$ is given by the formula

$$v_r(I) := q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^{n} (-1)^{r-s} q^{ms+\binom{r-s}{2}} \begin{bmatrix} n-s \\ n-r \end{bmatrix}_q \begin{bmatrix} n-i \\ s \end{bmatrix}_q .$$

Let $\mathscr{C}[I]$ be the space of matrices supported on $\{(i,i) \mid i \in I\}$.

Then $\mathscr{C}[I] \leq \mathbb{F}_q^{n \times m}$ is a linear rank-metric code, and

$$v_r(I) = W_r(\mathscr{C}[I]^\perp) = \frac{1}{|\mathscr{C}[I]|} \sum_{i=0}^{n} W_i(\mathscr{C}[I]) \sum_{s=0}^{n} (-1)^{j-s} q^{ms+\binom{j-s}{2}} \begin{bmatrix} n-i \\ s \end{bmatrix}_q \begin{bmatrix} n-s \\ j-s \end{bmatrix}_q .$$

Now, $|\mathscr{C}[I]| = q^{|I|}$ and $W_i(\mathscr{C}[I]) = \binom{|I|}{i}(q-1)^i$ for all i.

MacWilliams-type identities

MacWilliams-type identities have been extensively studied in the coding theory literature in various contexts:

- additive codes in finite abelian groups (discrete Fourier analysis),
- association schemes (Bose-Mesner algebras),
- regular lattices (support maps),
- posets (metric spaces from orders),
- ...

MacWilliams-type identities have been extensively studied in the coding theory literature in various contexts:

- additive codes in finite abelian groups (discrete Fourier analysis),
- association schemes (Bose-Mesner algebras),
- regular lattices (support maps),
- posets (metric spaces from orders),
- ...

Ingredients:

- a structured ambient space A
- a dual ambient space $\widehat{A}$
- a notion of duality: $\mathscr{C} \subseteq A$ yields $\mathscr{C}^\perp \subseteq \widehat{A}$
- counting devices on A and $\widehat{A}$ (e.g., the rank enumerator)

The pivot partition

For us, $A = \widehat{A} = \mathbb{F}_q^{n\times m}$. Duality is again trace-duality: $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ yields $\mathscr{C}^\perp \leq \mathbb{F}_q^{n\times m}$.

We partition the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form. This defines a partition $\mathscr{P}^{\mathrm{piv}}$ on $\mathbb{F}_q^{n\times m}$. Note:

$$|\mathscr{P}^{\mathrm{piv}}| = \sum_{r=0}^{n} \binom{m}{r}.$$

The pivot partition

For us, $A = \widehat{A} = \mathbb{F}_q^{n \times m}$. Duality is again trace-duality: $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ yields $\mathscr{C}^\perp \leq \mathbb{F}_q^{n \times m}$.

We partition the elements of $\mathbb{F}_q^{n \times m}$ according to the pivot indices in their reduced row-echelon form. This defines a partition $\mathscr{P}^{\mathrm{piv}}$ on $\mathbb{F}_q^{n \times m}$. Note:

$$|\mathscr{P}^{\mathrm{piv}}| = \sum_{r=0}^{n} \binom{m}{r}.$$

Example:

$$M = \begin{pmatrix} 1 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 1 & \bullet \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathrm{piv}(M) = (1, 3, 4).$$

The pivot partition

For us, $A = \widehat{A} = \mathbb{F}_q^{n\times m}$. Duality is again trace-duality: $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ yields $\mathscr{C}^\perp \le \mathbb{F}_q^{n\times m}$.

We partition the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form. This defines a partition $\mathscr{P}^{\mathrm{piv}}$ on $\mathbb{F}_q^{n\times m}$. Note:

$$|\mathscr{P}^{\mathrm{piv}}| = \sum_{r=0}^{n} \binom{m}{r}.$$

Example:

$$M = \begin{pmatrix} 1 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 1 & \bullet \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathrm{piv}(M) = (1,3,4).$$

Notation

$\Pi = \{(j_1,\dots,j_r) \mid 1 \le r \le n,\ \ 1 \le j_1 < j_2 < \cdots < j_r \le m\} \cup \{()\}$. Then $\mathscr{P}^{\mathrm{piv}} = (P_\lambda)_{\lambda \in \Pi}$.

For a code $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ and $\lambda \in \Pi$, $\mathscr{P}^{\mathrm{piv}}(\mathscr{C},\lambda) := |\mathscr{C} \cap P_\lambda|$.

The pivot partition

A MacWilliams identities for the pivot enumerator? Not exactly...

The pivot partition

A MacWilliams identities for the pivot enumerator? Not exactly...

$\mathscr{P}^{\text{rpiv}}$ partitions the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form **computed from the right**.

$$\mathscr{P}^{\text{rpiv}} = (Q_\mu)_{\mu\in\Pi}, \qquad \mathscr{P}^{\text{rpiv}}(\mathscr{C},\mu) := |\mathscr{C}\cap Q_\mu|.$$

Theorem (Gluesing-Luerssen, R.)

Let $\mathscr{C}\leq\mathbb{F}_q^{n\times m}$, and let $\lambda,\mu\in\Pi$. We have

$$\mathscr{P}^{\text{rpiv}}(\mathscr{C}^\perp,\mu) = \frac{1}{|\mathscr{C}|}\sum_{\lambda\in\Pi} K(\lambda,\mu)\cdot\mathscr{P}^{\text{piv}}(\mathscr{C},\lambda)$$

for suitable integers $K(\lambda,\mu)$. Moreover

$$(K(\lambda,\mu))_{\lambda,\mu}$$

is an invertible square matrix.

The pivot partition

A MacWilliams identities for the pivot enumerator? Not exactly...

$\mathscr{P}^{\mathrm{rpiv}}$ partitions the elements of $\mathbb{F}_q^{n\times m}$ according to the pivot indices in their reduced row-echelon form **computed from the right**.

$$\mathscr{P}^{\mathrm{rpiv}} = (Q_\mu)_{\mu\in\Pi}, \qquad \mathscr{P}^{\mathrm{rpiv}}(\mathscr{C},\mu) := |\mathscr{C}\cap Q_\mu|.$$

Theorem (Gluesing-Luerssen, R.)

Let $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$, and let $\lambda,\mu \in \Pi$. We have

$$\mathscr{P}^{\mathrm{rpiv}}(\mathscr{C}^\perp,\mu) = \frac{1}{|\mathscr{C}|}\sum_{\lambda\in\Pi} K(\lambda,\mu)\cdot \mathscr{P}^{\mathrm{piv}}(\mathscr{C},\lambda)$$

for suitable integers $K(\lambda,\mu)$. Moreover

$$(K(\lambda,\mu))_{\lambda,\mu}$$

is an invertible square matrix.

Computing $K(\lambda,\mu)$...

The pivot partition

Definition

A **Ferrers diagram** is a subset $\mathscr{F} \subseteq [n] \times [m]$ that satisfies the following:

1. if $(i,j) \in \mathscr{F}$ and $j < m$, then $(i,j+1) \in \mathscr{F}$ (right aligned),
2. if $(i,j) \in \mathscr{F}$ and $i > 1$, then $(i-1,j) \in \mathscr{F}$ (top aligned).

We represent a Ferrers diagram by its column lengths, $\mathscr{F} = [c_1, \ldots, c_m]$.

E.g.

$$\mathscr{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & & & \bullet \end{array} = [1,3,3,4]$$

The pivot partition

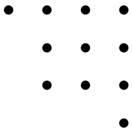
Definition

A **Ferrers diagram** is a subset $\mathscr{F} \subseteq [n] \times [m]$ that satisfies the following:

1. if $(i,j) \in \mathscr{F}$ and $j < m$, then $(i,j+1) \in \mathscr{F}$ (right aligned),
2. if $(i,j) \in \mathscr{F}$ and $i > 1$, then $(i-1,j) \in \mathscr{F}$ (top aligned).

We represent a Ferrers diagram by its column lengths, $\mathscr{F} = [c_1, \ldots, c_m]$.

E.g.

$\mathscr{F} =$  $= [1,3,3,4]$

We denote by $\mathbb{F}_q[\mathscr{F}]$ the space of matrices supported on $\mathscr{F}$, and let

$$P_r(\mathscr{F};q) := \{M \in \mathbb{F}_q[\mathscr{F}] \mid \mathrm{rk}(M) = r\}.$$

Definition

A **Ferrers diagram** is a subset $\mathscr{F} \subseteq [n] \times [m]$ that satisfies the following:

1. if $(i,j) \in \mathscr{F}$ and $j < m$, then $(i,j+1) \in \mathscr{F}$ (right aligned),
2. if $(i,j) \in \mathscr{F}$ and $i > 1$, then $(i-1,j) \in \mathscr{F}$ (top aligned).

We represent a Ferrers diagram by its column lengths, $\mathscr{F} = [c_1, \ldots, c_m]$.

E.g.

$$\mathscr{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & & & \bullet \end{array} = [1,3,3,4]$$

We denote by $\mathbb{F}_q[\mathscr{F}]$ the space of matrices supported on $\mathscr{F}$, and let

$$P_r(\mathscr{F};q) := \{M \in \mathbb{F}_q[\mathscr{F}] \mid \mathrm{rk}(M) = r\}.$$

We can express $K(\lambda,\mu)$ in terms of $P_r(\mathscr{F};q)$, for certain r and for a suitable diagram $\mathscr{F}$.

The pivot partition

Theorem (Gluesing-Luerssen, R.)

Let $\lambda, \mu \in \Pi$. Set

$$\sigma = [m] \setminus \mu, \qquad \lambda \cap \sigma = (\lambda_{\alpha_1}, \ldots, \lambda_{\alpha_x}), \qquad \mu \setminus \lambda = (\mu_{\beta_1}, \ldots, \mu_{\beta_y}).$$

Furthermore, set

$$z_j = |\{i \in [x] \mid \lambda_{\alpha_i} < \mu_{\beta_j}\}| \text{ for } j \in [y], \qquad \mathscr{F} = [z_1, \ldots, z_y].$$

The pivot partition

Theorem (Gluesing-Luerssen, R.)

Let $\lambda, \mu \in \Pi$. Set

$$\sigma = [m] \setminus \mu, \qquad \lambda \cap \sigma = (\lambda_{\alpha_1}, \dots, \lambda_{\alpha_x}), \qquad \mu \setminus \lambda = (\mu_{\beta_1}, \dots, \mu_{\beta_y}).$$

Furthermore, set

$$z_j = |\{i \in [x] \mid \lambda_{\alpha_i} < \mu_{\beta_j}\}| \;\text{ for } j \in [y], \qquad \mathscr{F} = [z_1, \dots, z_y].$$

Then

$$K(\lambda, \mu) \;=\; \sum_{t=0}^{m} (-1)^{|\lambda|-t} q^{nt+\binom{|\lambda|-t}{2}} \sum_{r=0}^{|\lambda\cap\sigma|} P_r(\mathscr{F}; q) \begin{bmatrix} |\lambda \cap \sigma| - r \\ t \end{bmatrix}_q .$$

The pivot partition

Theorem (Gluesing-Luerssen, R.)

Let $\lambda, \mu \in \Pi$. Set

$$\sigma = [m] \setminus \mu, \qquad \lambda \cap \sigma = (\lambda_{\alpha_1}, \ldots, \lambda_{\alpha_x}), \qquad \mu \setminus \lambda = (\mu_{\beta_1}, \ldots, \mu_{\beta_y}).$$

Furthermore, set

$$z_j = |\{i \in [x] \mid \lambda_{\alpha_i} < \mu_{\beta_j}\}| \text{ for } j \in [y], \qquad \mathscr{F} = [z_1, \ldots, z_y].$$

Then

$$K(\lambda,\mu) \; = \; \sum_{t=0}^{m} (-1)^{|\lambda|-t} q^{nt+\binom{|\lambda|-t}{2}} \sum_{r=0}^{|\lambda \cap \sigma|} P_r(\mathscr{F};q) \begin{bmatrix} |\lambda \cap \sigma| - r \\ t \end{bmatrix}_q .$$

Proof uses various techniques, including the notion of *regular support*...

(R., *Duality of Codes Supported on Regular Lattices, With an Application to Enumerative Combinatorics*, Des., Codes. and Crypt. 2017).

The pivot partition

Theorem (Gluesing-Luerssen, R.)

Let $\lambda, \mu \in \Pi$. Set

$$\sigma = [m] \setminus \mu, \qquad \lambda \cap \sigma = (\lambda_{\alpha_1}, \dots, \lambda_{\alpha_x}), \qquad \mu \setminus \lambda = (\mu_{\beta_1}, \dots, \mu_{\beta_y}).$$

Furthermore, set

$$z_j = |\{i \in [x] \mid \lambda_{\alpha_i} < \mu_{\beta_j}\}| \text{ for } j \in [y], \qquad \mathscr{F} = [z_1, \dots, z_y].$$

Then

$$K(\lambda, \mu) = \sum_{t=0}^{m} (-1)^{|\lambda|-t} q^{nt+\binom{|\lambda|-t}{2}} \sum_{r=0}^{|\lambda \cap \sigma|} P_r(\mathscr{F}; q) \begin{bmatrix} |\lambda \cap \sigma| - r \\ t \end{bmatrix}_q.$$

Proof uses various techniques, including the notion of *regular support*...

(R., *Duality of Codes Supported on Regular Lattices, With an Application to Enumerative Combinatorics*, Des., Codes. and Crypt. 2017).

$P_r(\mathscr{F}; q) \rightarrow$ **rook theory**

q-Rook Polynomials

Definition

The ***q*-rook polynomial** associated with $\mathscr{F}$ and $r \geq 0$ is

$$R_r(\mathscr{F}) = \sum_{C \in \mathrm{NAR}_r(\mathscr{F})} q^{\mathrm{inv}(C,\mathscr{F})} \in \mathbb{Z}[q],$$

where:

- $\mathrm{NAR}_r(\mathscr{F})$ is the set of all placements of r non-attacking rooks on $\mathscr{F}$ (non-attacking means that no two rooks are in the same column, and no two are in the same row)
- $\mathrm{inv}(C,\mathscr{F}) \in \mathbb{N}$ is computed as shown on the blackboard

Definition

The **q-rook polynomial** associated with $\mathscr{F}$ and $r \geq 0$ is

$$R_r(\mathscr{F}) = \sum_{C \in \mathrm{NAR}_r(\mathscr{F})} q^{\mathrm{inv}(C,\mathscr{F})} \in \mathbb{Z}[q],$$

where:

- $\mathrm{NAR}_r(\mathscr{F})$ is the set of all placements of r non-attacking rooks on $\mathscr{F}$ (non-attacking means that no two rooks are in the same column, and no two are in the same row)
- $\mathrm{inv}(C,\mathscr{F}) \in \mathbb{N}$ is computed as shown on the blackboard

Theorem (Haglund)

For any Ferrers diagram $\mathscr{F}$ and any $r \geq 0$ we have

$$P_r(\mathscr{F};q) = (q-1)^r \, q^{|\mathscr{F}|-r} \, R_r(\mathscr{F};q)_{|q^{-1}}$$

in the ring $\mathbb{Z}[q,q^{-1}]$.

Natural task: find an explicit expression for $R_r(\mathscr{F};q)$.

An explicit formula for $R_r(\mathscr{F})$:

Theorem (Gluesing-Luerssen, R.)

Let $\mathscr{F} = [c_1, \ldots, c_m]$ be an $n \times m$-Ferrers diagram. For $k \in [m]$ define $a_k = c_k - k + 1$.

For $j \in [m]$ let $\sigma_j \in \mathbb{Q}[x_1, \ldots, x_m]$ be the j^{th} elementary symmetric polynomial in m indeterminates ($\sigma_0 = 1$, ..., $\sigma_m = x_1 \cdots x_m$).

Then

$$R_r(\mathscr{F};q) = \frac{q^{\binom{r+1}{2} - rm + \text{area}(\mathscr{F})}(-1)^{m-r}}{(1-q)^r \prod_{k=1}^{m-r}(1-q^k)} \sum_{t=m-r}^{m} (-1)^t \sigma_{m-t}(q^{-a_1}, \ldots, q^{-a_m}) \prod_{j=0}^{m-r-1}(1-q^{t-j}).$$

An explicit formula for $R_r(\mathscr{F})$:

Theorem (Gluesing-Luerssen, R.)

Let $\mathscr{F} = [c_1, \dots, c_m]$ be an $n \times m$-Ferrers diagram. For $k \in [m]$ define $a_k = c_k - k + 1$.

For $j \in [m]$ let $\sigma_j \in \mathbb{Q}[x_1, \dots, x_m]$ be the j^{th} elementary symmetric polynomial in m indeterminates ($\sigma_0 = 1$, ..., $\sigma_m = x_1 \cdots x_m$).

Then

$$R_r(\mathscr{F}; q) = \frac{q^{\binom{r+1}{2} - rm + \text{area}(\mathscr{F})}(-1)^{m-r}}{(1-q)^r \prod_{k=1}^{m-r}(1-q^k)} \sum_{t=m-r}^{m} (-1)^t \sigma_{m-t}(q^{-a_1}, \dots, q^{-a_m}) \prod_{j=0}^{m-r-1}(1-q^{t-j}).$$

Combining this with Haglund's theorem we find an explicit expression for $P_r(\mathscr{F}; q)$.

Proof is technical.

A different approach: compute $P_r(\mathscr{F};q)$ directly. Notation: $\mathscr{F} = [c_1, \dots, c_m]$.

Theorem (Gluesing-Luerssen, R.)

$$P_r(\mathscr{F};q) = \sum_{1 \le i_1 < \dots < i_r \le m} q^{rm - \sum_{j=1}^r i_j} \prod_{j=1}^r (q^{c_{i_j} - j + 1} - 1).$$

Proof is short.

q-Rook Polynomials

A different approach: compute $P_r(\mathscr{F};q)$ directly. Notation: $\mathscr{F} = [c_1,\dots,c_m]$.

Theorem (Gluesing-Luerssen, R.)

$$P_r(\mathscr{F};q) = \sum_{1\leq i_1<\cdots<i_r\leq m} q^{rm-\sum_{j=1}^r i_j} \prod_{j=1}^r (q^{c_{i_j}-j+1}-1).$$

Proof is short.

But inverting Haglund's theorem we also find a simple explicit formula for $R_r(\mathscr{F};q)$!

Corollary (Gluesing-Luerssen, R.)

$$R_r(\mathscr{F};q) = \frac{q^{\sum_{j=1}^m c_j - rm} \displaystyle\sum_{1\leq i_1<\cdots<i_r\leq m} \prod_{j=1}^r (q^{i_j+j-c_{i_j}-1}-q^{i_j})}{(1-q)^r}.$$

q-Stirling Numbers

We can use these results to derive an explicit formula for the q-Stirling numbers of the second kind. The latter are defined via the recursion

$$S_{m+1,r} = q^{r-1} S_{m,r-1} + \frac{q^r - 1}{q - 1} S_{m,r}$$

with initial conditions $S_{0,0}(q) = 1$ and $S_{m,r}(q) = 0$ for $r < 0$ or $r > m$.

q-Stirling Numbers

We can use these results to derive an explicit formula for the q-Stirling numbers of the second kind. The latter are defined via the recursion

$$S_{m+1,r} = q^{r-1} S_{m,r-1} + \frac{q^r - 1}{q-1} S_{m,r}$$

with initial conditions $S_{0,0}(q) = 1$ and $S_{m,r}(q) = 0$ for $r < 0$ or $r > m$.

Theorem (Garsia, Remmel)

$$S_{m+1,m+1-r} = R_r(\mathscr{F}; q),$$

where $\mathscr{F} = [1, ..., m]$ is the upper-triangular $m \times m$ Ferrers board.

q-Stirling Numbers

We can use these results to derive an explicit formula for the q-Stirling numbers of the second kind. The latter are defined via the recursion

$$S_{m+1,r} = q^{r-1} S_{m,r-1} + \frac{q^r - 1}{q - 1} S_{m,r}$$

with initial conditions $S_{0,0}(q) = 1$ and $S_{m,r}(q) = 0$ for $r < 0$ or $r > m$.

Theorem (Garsia, Remmel)

$$S_{m+1,m+1-r} = R_r(\mathscr{F}; q),$$

where $\mathscr{F} = [1, \dots, m]$ is the upper-triangular $m \times m$ Ferrers board.

Theorem (Gluesing-Luerssen, R.)

$$S_{m+1,m+1-r} = \frac{q^{\binom{m+1}{2} - rm} \sum_{1 \le i_1 < \cdots < i_r \le m} \prod_{j=1}^{r} (q^{j-1} - q^{i_j})}{(1-q)^r} \quad \text{for } 1 \le r \le m+1.$$

q-Stirling Numbers

We can use these results to derive an explicit formula for the q-Stirling numbers of the second kind. The latter are defined via the recursion

$$S_{m+1,r} = q^{r-1} S_{m,r-1} + \frac{q^r - 1}{q-1} S_{m,r}$$

with initial conditions $S_{0,0}(q) = 1$ and $S_{m,r}(q) = 0$ for $r < 0$ or $r > m$.

Theorem (Garsia, Remmel)

$$S_{m+1,m+1-r} = R_r(\mathscr{F}; q),$$

where $\mathscr{F} = [1, \ldots, m]$ is the upper-triangular $m \times m$ Ferrers board.

Theorem (Gluesing-Luerssen, R.)

$$S_{m+1,m+1-r} = \frac{q^{\binom{m+1}{2} - rm} \displaystyle\sum_{1 \le i_1 < \cdots < i_r \le m} \prod_{j=1}^{r} (q^{j-1} - q^{i_j})}{(1-q)^r} \quad \text{for } 1 \le r \le m+1.$$

Thank you very much!