Network Coding and Equidistant Subspace Codes

Alberto Ravagnani

University College Dublin

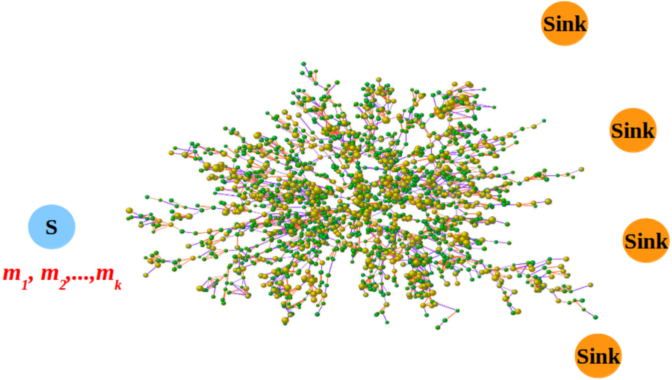
Ghent, December 5, 2017

What is network coding about?

Network coding: data transmission over (possibly noisy/adversarial) networks.

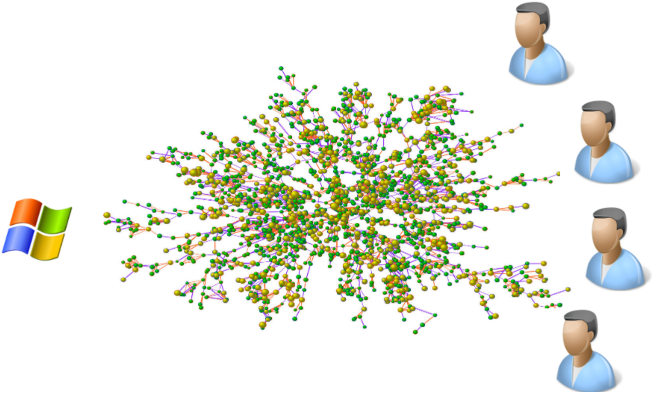
What is network coding about?

Network coding: data transmission over (possibly noisy/adversarial) networks.



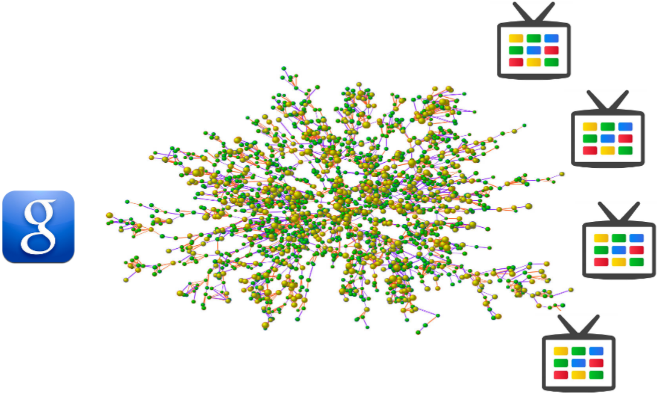
Applications of network coding

Patches distribution.



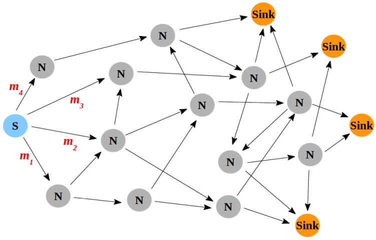
Applications of network coding

Streaming TV.



Modeling network communications

Network ⇝ directed acyclic multi-graph:



- The source  sends messages $m_1, m_2, \ldots, m_k \in \mathbb{F}_q^n$
- The sinks  demand **all** the messages (multicast)
- What about the nodes  ?

Goal

Maximize the amount of messages that can be delivered to **all** sinks per single channel use (**rate**).

KEY IDEA: allow the nodes to recombine messages before forwarding them towards the sinks.

Min-cut bound

- $\mathscr{N}$ the network
- $\mathbf{S}$ the source
- $\mathbf{R}_1, \ldots, \mathbf{R}_T$ the sinks (receivers)

Theorem (Ahlswede, Cai, Li, Yeung, 2000)

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

$$\text{rate} \leq \mu(\mathscr{N}) := \min_{i=1}^{T} \text{ min-cut}(\mathbf{S}, \mathbf{R}_i),$$

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

Min-cut bound

- $\mathscr{N}$ the network
- $\mathbf{S}$ the source
- $\mathbf{R}_1, \ldots, \mathbf{R}_T$ the sinks (receivers)

Theorem (Ahlswede, Cai, Li, Yeung, 2000)

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

$$\text{rate} \leq \mu(\mathscr{N}) := \min_{i=1}^{T} \text{ min-cut}(\mathbf{S}, \mathbf{R}_i),$$

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

Can we design nodes operations (**network code**) such that the bound is achieved?

Min-cut bound

- $\mathscr{N}$ the network
- $\mathbf{S}$ the source
- $\mathbf{R}_1, \ldots, \mathbf{R}_T$ the sinks (receivers)

Theorem (Ahlswede, Cai, Li, Yeung, 2000)

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

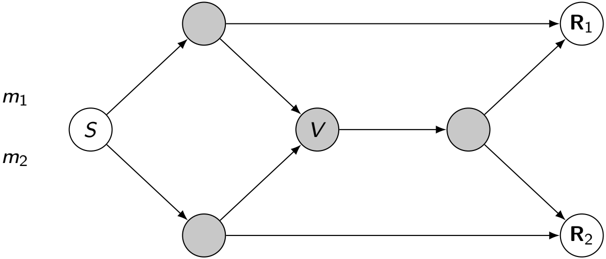
$$\text{rate} \leq \mu(\mathscr{N}) := \min_{i=1}^{T} \text{ min-cut}(\mathbf{S}, \mathbf{R}_i),$$

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

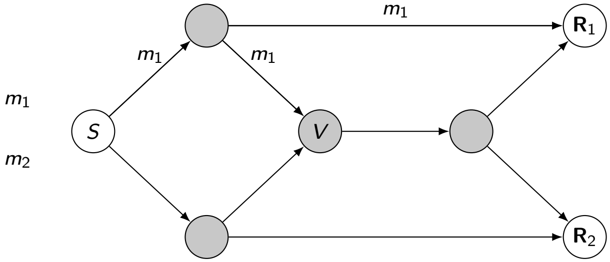
Can we design nodes operations (**network code**) such that the bound is achieved? YES!

In fact, **linear operations** suffice!

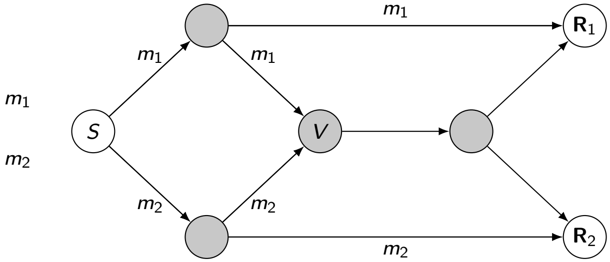
The "Butterfly" network



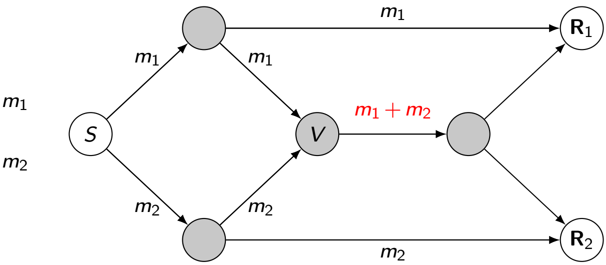
The "Butterfly" network



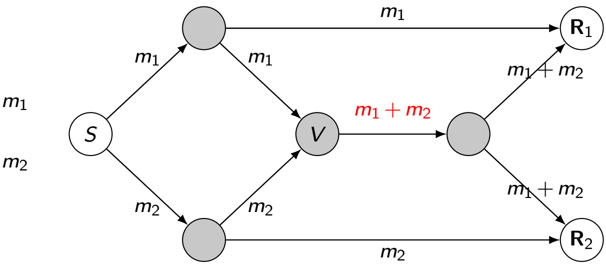
The "Butterfly" network



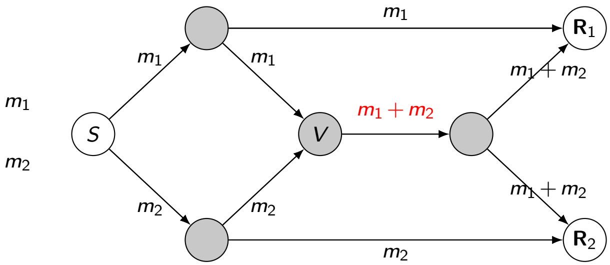
The "Butterfly" network



The “Butterfly” network



The "Butterfly" network



This strategy is optimal: there is no better strategy!

More generally...

Max-flow-min-cut theorem

Assume that:

- the source **S** sends messages $m_1, ..., m_k \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- the nodes forward the output of these operations,
- receiver **R** obtains vectors $n_1, ..., n_s$ on the incoming edges.

Max-flow-min-cut theorem

Assume that:

- the source **S** sends messages $m_1, \dots, m_k \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- the nodes forward the output of these operations,
- receiver **R** obtains vectors $n_1, \dots, n_s$ on the incoming edges.

Then we can write:

$$\begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_s \end{bmatrix} = G(\mathbf{R}) \cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{bmatrix},$$

where $G(\mathbf{R})$ is the **global transfer matrix** at **R**, describing all linear nodes operations.

Max-flow-min-cut theorem

Assume that:

- the source **S** sends messages $m_1, ..., m_k \in \mathbb{F}_q^n$,
- the nodes perform linear operations (**linear network coding**) on the received inputs,
- the nodes forward the output of these operations,
- receiver **R** obtains vectors $n_1, ..., n_s$ on the incoming edges.

Then we can write:

$$\begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_s \end{bmatrix} = G(\mathbf{R}) \cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{bmatrix},$$

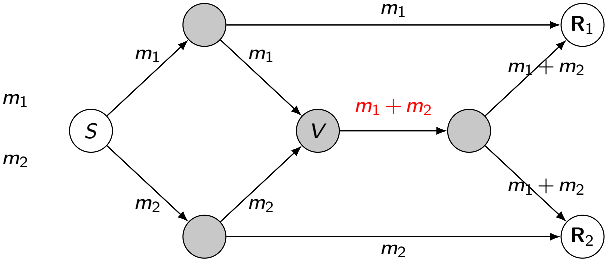
where $G(\mathbf{R})$ is the **global transfer matrix** at **R**, describing all linear nodes operations.

Theorem (Li, Yeung, Cai, 2002)

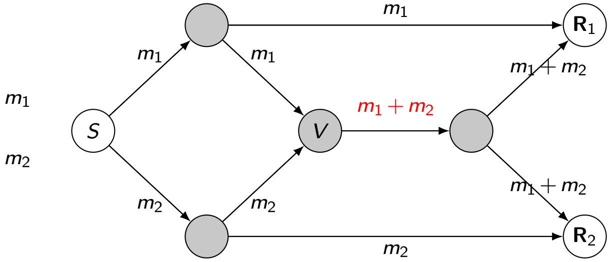
Assume $k = \mu(\mathcal{N})$. There exist linear nodes operations such that $G(\mathbf{R})$ is a $k \times k$ invertible matrix for each receiver **R**, provided that q is sufficiently large.

Network decoding at each receiver **R**: multiply by $G(\mathbf{R})^{-1}$.

Back to the Butterfly network



Back to the Butterfly network



Receiver $\mathbf{R}_1$ obtains

$$\begin{bmatrix} m_1 \\ m_1 + m_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}.$$

Thus

$$G(\mathbf{R}_1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Random network coding

Recall:

- the source organizes the messages $m_1, ..., m_k \in \mathbb{F}_q^n$ in the rows of a **message matrix** M,
- if no errors occur, then receiver $\mathbf{R}$ obtains $Y = G(\mathbf{R}) \cdot M$.

If the network $\mathscr{N}$ is large, or time-dependent, then the $G(\mathbf{R})$'s may be difficult to design.

Random network coding

Recall:

- the source organizes the messages $m_1, \ldots, m_k \in \mathbb{F}_q^n$ in the rows of a **message matrix** M,
- if no errors occur, then receiver $\mathbf{R}$ obtains $Y = G(\mathbf{R}) \cdot M$.

If the network $\mathcal{N}$ is large, or time-dependent, then the $G(\mathbf{R})$'s may be difficult to design.

Theorem (Ho, Médard, Kötter, Karger, Effros, Shi, Leong, 2006)

Assume $k = \mu(\mathcal{N})$. If each node performs **random** linear operations on the received inputs, then

$$\lim_{q \to \infty} \mathbb{P}[G(\mathbf{R}) \text{ is left-invertible for all } \mathbf{R}] = 1.$$

Random network coding

Recall:

- the source organizes the messages $m_1, \dots, m_k \in \mathbb{F}_q^n$ in the rows of a **message matrix** M,
- if no errors occur, then receiver $\mathbf{R}$ obtains $Y = G(\mathbf{R}) \cdot M$.

If the network $\mathscr{N}$ is large, or time-dependent, then the $G(\mathbf{R})$'s may be difficult to design.

Theorem (Ho, Médard, Kötter, Karger, Effros, Shi, Leong, 2006)

Assume $k = \mu(\mathscr{N})$. If each node performs **random** linear operations on the received inputs, then

$$\lim_{q \to \infty} \mathbb{P}[G(\mathbf{R}) \text{ is left-invertible for all } \mathbf{R}] = 1.$$

If $G(\mathbf{R})$ is left-invertible, what do M and $G(\mathbf{R}) \cdot M$ have in common? The row-space!

IDEA (Kötter, Kschischang, 2008): define the message to be $\text{rowsp}(M)$.

Random network coding

Recall:

- the source organizes the messages $m_1, \ldots, m_k \in \mathbb{F}_q^n$ in the rows of a **message matrix** M,
- if no errors occur, then receiver $\mathbf{R}$ obtains $Y = G(\mathbf{R}) \cdot M$.

If the network $\mathscr{N}$ is large, or time-dependent, then the $G(\mathbf{R})$'s may be difficult to design.

Theorem (Ho, Médard, Kötter, Karger, Effros, Shi, Leong, 2006)

Assume $k = \mu(\mathscr{N})$. If each node performs **random** linear operations on the received inputs, then

$$\lim_{q \to \infty} \mathbb{P}[G(\mathbf{R}) \text{ is left-invertible for all } \mathbf{R}] = 1.$$

If $G(\mathbf{R})$ is left-invertible, what do M and $G(\mathbf{R}) \cdot M$ have in common? The row-space!

IDEA (Kötter, Kschischang, 2008): define the message to be $\mathrm{rowsp}(M)$.

$1 \leq k < n$ integers, q prime power, $\mathscr{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition

A **subspace code** of length n and dimension k is a subset $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$.
The elements of $\mathscr{C}$ are the "legitimate" message spaces.

Codes for networks

$1 \leq k < n$ integers, q prime power, $\mathscr{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition (Kötter-Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

Codes for networks

$1 \leq k < n$ integers, q prime power, $\mathscr{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition (Kötter-Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

Goal of communication scheme

Message transmission + Error correction.

(1) $V = \text{Span}_{\mathbb{F}_q}\{m_1, m_2, ..., m_k\} \in \mathscr{C}$ is sent...

Codes for networks

$1 \leq k < n$ integers, q prime power, $\mathcal{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

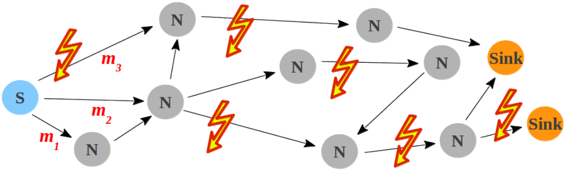
Definition (Kötter-Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathcal{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

Goal of communication scheme

Message transmission $+$ Error correction.

(1) $V = \mathrm{Span}_{\mathbb{F}_q}\{m_1, m_2, \dots, m_k\} \in \mathscr{C}$ is sent...



(2) ...$V \oplus E$ is received, $E \subseteq \mathbb{F}_q^n$ subspace $\rightsquigarrow$ **number** of errors $:= \dim_{\mathbb{F}_q}(E)$.

Decoding: recover V from $V \oplus E$.

Subspace codes

$1 \leq k < n$ integers, q prime power, $\mathscr{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition (Kötter, Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

Subspace codes

$1 \leq k < n$ integers, q prime power, $\mathcal{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition (Kötter, Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathcal{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

(1) **Subspace distance** on $\mathcal{G}_q(k,n)$: $d(V,W) := 2k - 2\dim(V \cap W)$, $V,W \in \mathcal{G}_q(k,n)$.

(2) **Minimum distance** of $\mathscr{C} \subseteq \mathcal{G}_q(k,n)$: $d(\mathscr{C}) := \min\{d(V,W) : V,W \in \mathscr{C}, V \neq W\}$.

Subspace codes

$1 \leq k < n$ integers, q prime power, $\mathcal{G}_q(k,n)$ set of k-dimensional subspaces of $\mathbb{F}_q^n$.

Definition (Kötter, Kschischang, 2008)

A **subspace code** is a subset $\mathscr{C} \subseteq \mathcal{G}_q(k,n)$ with $|\mathscr{C}| \geq 2$. Elements of $\mathscr{C}$: **codewords**.

(1) **Subspace distance** on $\mathcal{G}_q(k,n)$: $d(V,W) := 2k - 2\dim(V \cap W)$, $V, W \in \mathcal{G}_q(k,n)$.

(2) **Minimum distance** of $\mathscr{C} \subseteq \mathcal{G}_q(k,n)$: $d(\mathscr{C}) := \min\{d(V,W) : V, W \in \mathscr{C}, V \neq W\}$.

... new research directions in Coding Theory:

- Bounds on the cardinality of subspace codes (for given minimum distance).
- Construction of subspace codes.
- Decoding algorithms.
- Connections to Projective Geometry.
- Applications to Cryptography.

Bounds and constructions

Singleton-type bound:

Theorem

Assume $n \geq 2k$. Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a subspace code of minimum distance $d(\mathscr{C}) = 2\delta$. Then

$$|\mathscr{C}| < 4 \cdot q^{(n-k)(k-\delta+1)}.$$

Singleton-type bound:

Theorem

Assume $n \geq 2k$. Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a subspace code of minimum distance $d(\mathscr{C}) = 2\delta$. Then

$$|\mathscr{C}| < 4 \cdot q^{(n-k)(k-\delta+1)}.$$

Reed-Solomon-like codes:

Theorem

Assume $n \geq 2k$. For every $1 \leq \delta \leq k$ there exists a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ of minimum distance $d(\mathscr{C}) = 2\delta$ and

$$|\mathscr{C}| = q^{(n-k)(k-\delta+1)}.$$

Bounds and constructions

Singleton-type bound:

Theorem

Assume $n \geq 2k$. Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a subspace code of minimum distance $d(\mathscr{C}) = 2\delta$. Then

$$|\mathscr{C}| < 4 \cdot q^{(n-k)(k-\delta+1)}.$$

Reed-Solomon-like codes:

Theorem

Assume $n \geq 2k$. For every $1 \leq \delta \leq k$ there exists a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ of minimum distance $d(\mathscr{C}) = 2\delta$ and

$$|\mathscr{C}| = q^{(n-k)(k-\delta+1)}.$$

Reed-Solomon-like codes are optimal, up to constant factor.

Efficient decoding algorithms are known.

Equidistant subspace codes

Definition

A subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is **equidistant** is $d(V,W)$ is constant for all $V \neq W \in \mathscr{C}$.

I.e., $c := \dim(V \cap W)$ is constant ($\mathscr{C}$ is c-**intersecting**).

Equidistant subspace codes

Definition

A subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is **equidistant** is $d(V,W)$ is constant for all $V \neq W \in \mathscr{C}$.

I.e., $c := \dim(V \cap W)$ is constant ($\mathscr{C}$ is c-**intersecting**).

Problems

1. Describe properties of large equidistant codes.
2. Construct large sets of equidistant codes (and decode them).

Equidistant subspace codes

Definition

A subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is **equidistant** is $d(V,W)$ is constant for all $V \neq W \in \mathscr{C}$.

I.e., $c := \dim(V \cap W)$ is constant ($\mathscr{C}$ is c-**intersecting**).

Problems

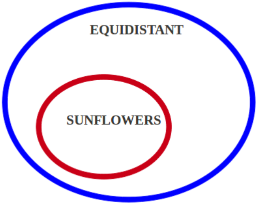
1. Describe properties of large equidistant codes.
2. Construct large sets of equidistant codes (and decode them).

Focus on: **asymptotic/general** structural properties.

Sunflowers

Definition

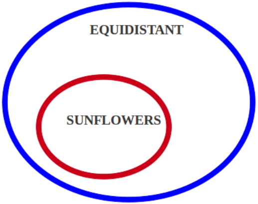
An equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is a **sunflower** if there is $C \subseteq \mathbb{F}_q^n$ st. $V \cap W = C$ for all $V \neq W \in \mathscr{C}$. The space C is the **center**.



Sunflowers

Definition

An equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is a **sunflower** if there is $C \subseteq \mathbb{F}_q^n$ st. $V \cap W = C$ for all $V \neq W \in \mathscr{C}$. The space C is the **center**.



Theorem (Deza, Etzion-Raviv)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a c-intersecting equidistant codes. Assume

$$|\mathscr{C}| \geq \left(\frac{q^k - q^c}{q-1}\right)^2 + \frac{q^k - q^c}{q-1} + 1.$$

Then $\mathscr{C}$ is a sunflower.

Sunflowers and partial spreads

Definition

A **partial** k**-spread** in $\mathbb{F}_q^n$ is a set $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ such that $U \cap V = \{0\}$ for all $U, V \in \mathscr{C}$ with $U \neq V$.

There exists a 1-to-1 correspondence:

$$c\text{-intersecting sunflowers in } \mathbb{F}_q^n \quad \leftrightsquigarrow \quad \text{partial } (k-c)\text{-spreads in } \mathbb{F}_q^{n-c}$$

Proposition (Gorla, R.)

Let $e_q(k,n,c) := \max\{|\mathscr{C}| \, : \, \mathscr{C} \subseteq \mathscr{G}_q(k,n) \text{ is a sunflower with center of dimension } c\}$.
Denote by r be the reminder of the division of $n-c$ by $k-c$.

Then:

$$\frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1 \;\leq\; e_q(k,n,c) \;\leq\; \frac{q^{n-c}-q^r}{q^{k-c}-1}.$$

Classification of sunflower codes

We classify equidistant codes of **maximum cardinality** for most values of the parameters.

Definition

Denote by $V^\perp$ the orthogonal of a subspace $V \subseteq \mathbb{F}_q^n$ w.r. to the standard inner product of $\mathbb{F}_q^n$. The **orthogonal** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $\mathscr{C}^\perp := \{V^\perp : V \in \mathscr{C}\}$.

Classification of sunflower codes

We classify equidistant codes of **maximum cardinality** for most values of the parameters.

Definition

Denote by $V^\perp$ the orthogonal of a subspace $V \subseteq \mathbb{F}_q^n$ w.r. to the standard inner product of $\mathbb{F}_q^n$.
The **orthogonal** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $\mathscr{C}^\perp := \{V^\perp : V \in \mathscr{C}\}$.

Theorem (Gorla, R.)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume that at least one of the following holds:

- $c \in \{0, k-1, 2k-n\}$,
- $q \gg 0$ and $n \geq 3k-1$,
- $q \gg 0$ and $n \leq (3k+1)/2$.

Then either $\mathscr{C}$ is a sunflower, or $\mathscr{C}^\perp$ is a sunflower (mutually exclusive properties).

Classification of sunflower codes

We classify equidistant codes of **maximum cardinality** for most values of the parameters.

Definition

Denote by $V^\perp$ the orthogonal of a subspace $V \subseteq \mathbb{F}_q^n$ w.r. to the standard inner product of $\mathbb{F}_q^n$.
The **orthogonal** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $\mathscr{C}^\perp := \{V^\perp : V \in \mathscr{C}\}$.

Theorem (Gorla, R.)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume that at least one of the following holds:

- $c \in \{0, k-1, 2k-n\}$,
- $q \gg 0$ and $n \geq 3k-1$,
- $q \gg 0$ and $n \leq (3k+1)/2$.

Then either $\mathscr{C}$ is a sunflower, or $\mathscr{C}^\perp$ is a sunflower (mutually exclusive properties).

There are counterexamples in the range $(3k+1)/2 < n < 3k-1$ for all q, e.g.

Proposition (Gorla, R.)

An equidistant 1-intersecting code $\mathscr{C} \subseteq \mathscr{G}_q(3,6)$ of maximum cardinality is **never** a sunflower.

Construction of sunflower codes

$p \in \mathbb{F}_q[x]$ irreducible, monic; $k := \deg(p)$; $p = \sum_{i=0}^{k} p_i x^i$. **Companion matrix** of p:

$$\mathrm{M}(p) := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{bmatrix}.$$

We have $\mathbb{F}_q[M(p)] \cong \mathbb{F}_{q^k}$.

Construction of sunflower codes

Theorem

- Take integers $1 \leq k < n$ and $\min\{0, 2k-n\} \leq c \leq k-1$.
- Write $n - c = h(k-c) + r$, with $0 \leq r \leq k-c-1$ and $h \geq 2$.
- Choose irreducible monic polynomials $p, p' \in \mathbb{F}_q[x]$ of degree $k-c$ and $k-c+r$, resp.
- Set $P := \mathrm{M}(p)$ and $P' := \mathrm{M}(p')$.
- For $1 \leq i \leq h-1$ let $\mathscr{M}_i(p,p')$ be the set of $k \times n$ matrices of the form

$$\begin{bmatrix} I_c & 0_{c\times(k-c)} & \cdots & \cdots & \cdots & \cdots & \cdots & 0_{c\times(k-c)} & 0_{c\times(k-c+r)} \\ 0_{(k-c)\times c} & 0_{k-c} & \cdots & 0_{k-c} & I_{k-c} & A_{i+1} & \cdots & A_{h-1} & A_{[k-c]} \end{bmatrix},$$

  where we have $i-2$ consecutive copies of 0_{k-c}, $A_{i+1}, \dots, A_{h-1} \in \mathbb{F}_q[P]$, $A \in \mathbb{F}_q[P']$, and $A_{[k-c]}$ denotes the last $k-c$ rows of A.

The set

$$\mathscr{C} := \bigcup_{i=1}^{h-1} \{\mathrm{rowsp}(M) : M \in \mathscr{M}_i(p,p')\} \cup \left\{ \mathrm{rowsp} \begin{bmatrix} I_c & 0_{c\times(k-c)} & \cdots & 0_{c\times(k-c)} & 0_{c\times(k-c+r)} & 0_{c\times(k-c)} \\ 0_{(k-c)\times c} & 0_{k-c} & \cdots & 0_{k-c} & 0_{(k-c)\times(k-c+r)} & I_{k-c} \end{bmatrix} \right\}$$

is a sunflower in $\mathscr{G}_q(k,n)$ of cardinality $|\mathscr{C}| = \frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1$.

Theorem

Sunflower codes:

1. have **efficient decoding algorithm**,
2. are **asymptotically optimal** as sunflowers, and therefore as equidistant codes for most parameters (classification).

Sunflower codes

Theorem

Sunflower codes:

1. have **efficient decoding algorithm**,
2. are **asymptotically optimal** as sunflowers, and therefore as equidistant codes for most parameters (classification).

Other problems we investigated

1. Classify optimal equidistant codes $\mathscr{C}$ such that both $\mathscr{C}$ and $\mathscr{C}^{\perp}$ are sunflowers.
2. Estimate the number of distinct intersections of a non-sunflower equidistant codes.

Sunflower codes

Theorem

Sunflower codes:

1. have **efficient decoding algorithm**,
2. are **asymptotically optimal** as sunflowers, and therefore as equidistant codes for most parameters (classification).

Other problems we investigated

1. Classify optimal equidistant codes $\mathscr{C}$ such that both $\mathscr{C}$ and $\mathscr{C}^\perp$ are sunflowers.
2. Estimate the number of distinct intersections of a non-sunflower equidistant codes.

Recall...

Theorem (Gorla, R.)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume that at least one of the following holds:

- $c \in \{0, k-1, 2k-n\}$,
- $q \gg 0$ and $n \geq 3k-1$,
- $q \gg 0$ and $n \leq (3k+1)/2$.

Then either $\mathscr{C}$ is a sunflower, or $\mathscr{C}^\perp$ is a sunflower (mutually exclusive properties).

More properties of equidistant codes

Define the **span** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ as $\text{span}(\mathscr{C}) := \sum_{U \in \mathscr{C}} U \quad \subseteq \mathbb{F}_q^n$.

Lemma

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant code of maximum cardinality. Then $\text{span}(\mathscr{C}) = \mathbb{F}_q^n$.

More properties of equidistant codes

Define the **span** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ as $\text{span}(\mathscr{C}) := \sum_{U \in \mathscr{C}} U \quad \subseteq \mathbb{F}_q^n$.

Lemma

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant code of maximum cardinality. Then $\text{span}(\mathscr{C}) = \mathbb{F}_q^n$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume $n > 2k - c$. Then $\mathscr{C}^\perp$ is **not** a sunflower.

More properties of equidistant codes

Define the **span** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ as $\text{span}(\mathscr{C}) := \sum_{U \in \mathscr{C}} U \quad \subseteq \mathbb{F}_q^n$.

Lemma

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant code of maximum cardinality. Then $\text{span}(\mathscr{C}) = \mathbb{F}_q^n$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume $n > 2k - c$. Then $\mathscr{C}^\perp$ is **not** a sunflower.

1. Assume that $\mathscr{C}^\perp$ is a sunflower. The center of $\mathscr{C}^\perp$, say D, has $\dim(D) = n - 2k + c > 0$.
2. We have $U^\perp \supseteq D$ for all $U \in \mathscr{C}$, and thus $U \subseteq D^\perp$ for all $U \in \mathscr{C}$.
3. It follows $\text{span}(\mathscr{C}) \subseteq D^\perp \subsetneq \mathbb{F}_q^n$, contradicting the lemma.

More properties of equidistant codes

Define the **span** of a subspace code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ as $\text{span}(\mathscr{C}) := \sum_{U \in \mathscr{C}} U \quad \subseteq \mathbb{F}_q^n$.

Lemma

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant code of maximum cardinality. Then $\text{span}(\mathscr{C}) = \mathbb{F}_q^n$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an equidistant c-intersecting code of maximum cardinality. Assume $n > 2k - c$. Then $\mathscr{C}^\perp$ is **not** a sunflower.

1. Assume that $\mathscr{C}^\perp$ is a sunflower. The center of $\mathscr{C}^\perp$, say D, has $\dim(D) = n - 2k + c > 0$.
2. We have $U^\perp \supseteq D$ for all $U \in \mathscr{C}$, and thus $U \subseteq D^\perp$ for all $U \in \mathscr{C}$.
3. It follows $\text{span}(\mathscr{C}) \subseteq D^\perp \subsetneq \mathbb{F}_q^n$, contradicting the lemma.

Corollary

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a c-intersecting equidistant code of maximum cardinality. TFAE:

- $\mathscr{C}$ and $\mathscr{C}^\perp$ are both sunflowers,
- $c = 0$ and $n = 2k$,
- $n = 2k$ and both $\mathscr{C}$ and $\mathscr{C}^\perp$ are spreads.

Centers of equidistant codes

The **set of centers** of an equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $T(\mathscr{C}) := \{U \cap V \ : \ U, V \in \mathscr{C}, \ U \neq V\}$, and the **number of centers** of $\mathscr{C}$ is $t(\mathscr{C}) := |T(\mathscr{C})|$.

Centers of equidistant codes

The **set of centers** of an equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $T(\mathscr{C}) := \{U \cap V \ : \ U, V \in \mathscr{C},\ U \neq V\}$, and the **number of centers** of $\mathscr{C}$ is $t(\mathscr{C}) := |T(\mathscr{C})|$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an c-intersecting equidistant code. One of the following properties holds:

1. $\mathscr{C}$ is a sunflower, or
2. $t(\mathscr{C}) \geq |\mathscr{C}| \frac{q^c - q^{c-1}}{q^k - q^{c-1}}$.

Centers of equidistant codes

The **set of centers** of an equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $T(\mathscr{C}) := \{U \cap V \ : \ U,V \in \mathscr{C},\ U \neq V\}$, and the **number of centers** of $\mathscr{C}$ is $t(\mathscr{C}) := |T(\mathscr{C})|$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an c-intersecting equidistant code. One of the following properties holds:

1. $\mathscr{C}$ is a sunflower, or
2. $t(\mathscr{C}) \geq |\mathscr{C}| \frac{q^c - q^{c-1}}{q^k - q^{c-1}}$.

Corollary (asymptotic estimate of the number of centers)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a c-intersecting non-sunflower equidistant code of maximum cardinality. Denote by r the remainder of the division of $n-c$ by $k-c$. Then

$$t(\mathscr{C}) \geq \left(\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}}.$$

In particular, $\lim_{q \to \infty} t(\mathscr{C}) q^{-(n-2k+c)} \in [1, +\infty]$.

Centers of equidistant codes

The **set of centers** of an equidistant code $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ is $T(\mathscr{C}) := \{U \cap V \ : \ U, V \in \mathscr{C},\ U \neq V\}$, and the **number of centers** of $\mathscr{C}$ is $t(\mathscr{C}) := |T(\mathscr{C})|$.

Proposition

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be an c-intersecting equidistant code. One of the following properties holds:

1. $\mathscr{C}$ is a sunflower, or
2. $t(\mathscr{C}) \geq |\mathscr{C}| \frac{q^c - q^{c-1}}{q^k - q^{c-1}}$.

Corollary (asymptotic estimate of the number of centers)

Let $\mathscr{C} \subseteq \mathscr{G}_q(k,n)$ be a c-intersecting non-sunflower equidistant code of maximum cardinality. Denote by r the remainder of the division of $n-c$ by $k-c$. Then

$$t(\mathscr{C}) \geq \left(\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}}.$$

In particular, $\lim_{q \to \infty} t(\mathscr{C}) q^{-(n-2k+c)} \in [1, +\infty]$.

Thank you very much for your attention!