Covering Radius of Rank-Metric Codes

Alberto Ravagnani

– University College Dublin –

MTNS 18, Hong Kong, July 2018

joint work with Eimear Byrne

Rank-metric codes

Definition

A (**rank-metric**) **code** is a non-empty subset $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$. We assume $n \le m$ w.l.o.g.

The (**rank**) **distance** between matrices $M, N \in \mathbb{F}_q^{n \times m}$ is $\mathrm{rk}(M - N)$.

If $|\mathscr{C}| \ge 2$, then the **minimum distance** of $\mathscr{C}$ is

$$d(\mathscr{C}) := \min\{\mathrm{rk}(M - N) \mid M, N \in \mathscr{C},\, M \neq N\}.$$

Definition

A (**rank-metric**) **code** is a non-empty subset $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$. We assume $n \leq m$ w.l.o.g.

The (**rank**) **distance** between matrices $M, N \in \mathbb{F}_q^{n\times m}$ is $\mathrm{rk}(M-N)$.

If $|\mathscr{C}| \geq 2$, then the **minimum distance** of $\mathscr{C}$ is

$$d(\mathscr{C}) := \min\{\mathrm{rk}(M-N) \mid M, N \in \mathscr{C}, M \neq N\}.$$

We say that $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is **linear** if it is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$. In this case the **dual** of $\mathscr{C}$ is the linear code

$$\mathscr{C}^\perp := \{N \in \mathbb{F}_q^{n\times m} : \mathrm{Tr}(MN^t) = 0 \text{ for all } M \in \mathscr{C}\} \subseteq \mathbb{F}_q^{n\times m}.$$

Rank-metric codes

Definition

A (**rank-metric**) **code** is a non-empty subset $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$. We assume $n \leq m$ w.l.o.g.

The (**rank**) **distance** between matrices $M, N \in \mathbb{F}_q^{n\times m}$ is $\mathrm{rk}(M-N)$.

If $|\mathscr{C}| \geq 2$, then the **minimum distance** of $\mathscr{C}$ is

$$d(\mathscr{C}) := \min\{\mathrm{rk}(M-N) \mid M, N \in \mathscr{C},\, M \neq N\}.$$

We say that $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is **linear** if it is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$. In this case the **dual** of $\mathscr{C}$ is the linear code

$$\mathscr{C}^\perp := \{N \in \mathbb{F}_q^{n\times m} : \mathrm{Tr}(MN^t) = 0 \text{ for all } M \in \mathscr{C}\} \subseteq \mathbb{F}_q^{n\times m}.$$

- Studied by Delsarte for combinatorial interest via association schemes.
- Further studied independently by Gabidulin and Roth.
- Re-discovered by Kötter, Kschischang, Silva and applied to linear network coding.

Rank-metric codes

Definition

A (**rank-metric**) **code** is a non-empty subset $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$. We assume $n \leq m$ w.l.o.g.

The (**rank**) **distance** between matrices $M, N \in \mathbb{F}_q^{n\times m}$ is $\mathrm{rk}(M-N)$.

If $|\mathscr{C}| \geq 2$, then the **minimum distance** of $\mathscr{C}$ is

$$d(\mathscr{C}) := \min\{\mathrm{rk}(M-N) \mid M, N \in \mathscr{C},\, M \neq N\}.$$

We say that $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is **linear** if it is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$. In this case the **dual** of $\mathscr{C}$ is the linear code

$$\mathscr{C}^\perp := \{N \in \mathbb{F}_q^{n\times m} : \mathrm{Tr}(MN^t) = 0 \text{ for all } M \in \mathscr{C}\} \subseteq \mathbb{F}_q^{n\times m}.$$

- Studied by Delsarte for combinatorial interest via association schemes.
- Further studied independently by Gabidulin and Roth.
- Re-discovered by Kötter, Kschischang, Silva and applied to linear network coding.

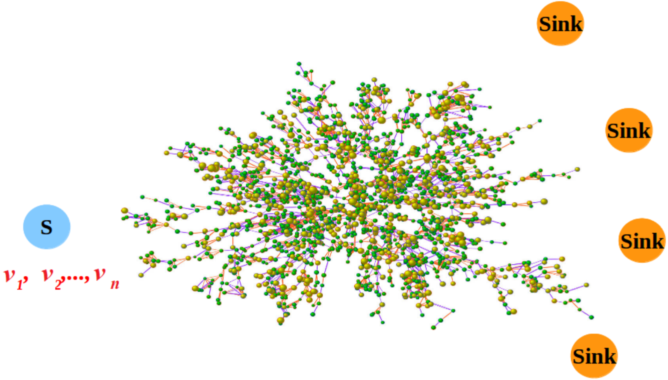
What is linear network coding?

What is network coding about?

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

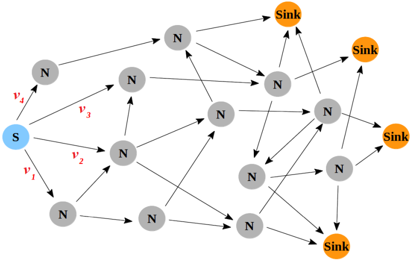
What is network coding about?

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



A model for network communications

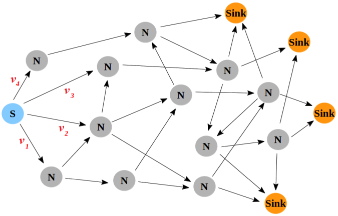
Network $\rightsquigarrow$ directed acyclic multi-graph:



- The source (S) sends messages $v_1, v_2, \dots, v_n \in \mathbb{F}_q^m$
- The sinks (Sink) demand **all** the messages (multicast)
- The nodes (N) forward linear combinations of the received inputs.

Rank-metric codes allow error correction in this context.

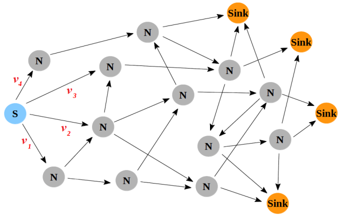
A model for network communications



Organize $v_1, \dots, v_n$ as the rows of a matrix $M := \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{F}_q^{n\times m}$.

Measure the **distance** between $M, N \in \mathbb{F}_q^{n\times m}$ as $\mathrm{rk}(M - N)$.

A model for network communications

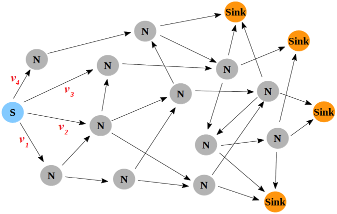


Organize $v_1, \dots, v_n$ as the rows of a matrix $M := \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{F}_q^{n \times m}$.

Measure the **distance** between $M, N \in \mathbb{F}_q^{n \times m}$ as $\mathrm{rk}(M - N)$.

Why does this make sense?

A model for network communications



Organize $v_1, \ldots, v_n$ as the rows of a matrix $M := \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{F}_q^{n \times m}$.

Measure the **distance** between $M, N \in \mathbb{F}_q^{n \times m}$ as $\mathrm{rk}(M - N)$.

Why does this make sense?

Silva, Kschishang, *On metrics for error correction in network coding*. IEEE Tran. IT, '09.

A model for network communications

R., Kschischang, *Adversarial network coding*. IEEE Tran. IT, '18.

- Mathematical framework for network coding with adversar**ies** of different types.
- Rigorous definition of adversarial capacit**ies** of a network.
- Various communication models.
- Difference between "code" and "network code" and separability results.
- One source vs. multiple sources (interference).
- Techniques to prove bounds.
- Constructions.
- Open problems.

Covering Radius

Back to the mathematical theory of rank-metric codes...

Byrne, R., *Covering radius of matrix codes endowed with the rank metric*. SIAM J. Discrete Math. '17.

Byrne, R., *Partition-balanced families of codes and density problems in coding theory*. Preprint '18.

Definition

The **covering radius** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is the integer

$$\rho(\mathscr{C}) := \min\{i \in \mathbb{N} \mid \text{for all } X \in \mathbb{F}_q^{n\times m} \text{ there exists } M \in \mathscr{C} \text{ with } d(X,M) \leq i\}$$

Covering Radius

Back to the mathematical theory of rank-metric codes...

Byrne, R., *Covering radius of matrix codes endowed with the rank metric*. SIAM J. Discrete Math. '17.

Byrne, R., *Partition-balanced families of codes and density problems in coding theory*. Preprint '18.

Definition

The **covering radius** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ is the integer

$$\rho(\mathscr{C}) := \min\{i \in \mathbb{N} \mid \text{for all } X \in \mathbb{F}_q^{n \times m} \text{ there exists } M \in \mathscr{C} \text{ with } d(X, M) \leq i\}$$

This the rank-analogue of the covering radius of a code $C \subseteq \mathbb{F}_q^n$ endowed with the Hamming distance.

Covering Radius

Back to the mathematical theory of rank-metric codes...

Byrne, R., *Covering radius of matrix codes endowed with the rank metric*. SIAM J. Discrete Math. '17.

Byrne, R., *Partition-balanced families of codes and density problems in coding theory*. Preprint '18.

Definition

The **covering radius** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ is the integer

$$\rho(\mathscr{C}) := \min\{i \in \mathbb{N} \mid \text{for all } X \in \mathbb{F}_q^{n \times m} \text{ there exists } M \in \mathscr{C} \text{ with } d(X, M) \leq i\}$$

This the rank-analogue of the covering radius of a code $C \subseteq \mathbb{F}_q^n$ endowed with the Hamming distance.

$\rho(\mathscr{C})$ is the minimum value r such that the union of the spheres of radius r about the codeword cover the ambient space.

Covering Radius

Back to the mathematical theory of rank-metric codes...

Byrne, R., *Covering radius of matrix codes endowed with the rank metric*. SIAM J. Discrete Math. '17.

Byrne, R., *Partition-balanced families of codes and density problems in coding theory*. Preprint '18.

Definition

The **covering radius** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is the integer

$$\rho(\mathscr{C}) := \min\{i \in \mathbb{N} \mid \text{for all } X \in \mathbb{F}_q^{n\times m} \text{ there exists } M \in \mathscr{C} \text{ with } d(X,M) \leq i\}$$

This the rank-analogue of the covering radius of a code $C \subseteq \mathbb{F}_q^n$ endowed with the Hamming distance.

$\rho(\mathscr{C})$ is the minimum value r such that the union of the spheres of radius r about the codeword cover the ambient space.

APPLICATIONS: error correction, index coding, source coding.

First properties of the covering radius

Lemma

Let $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ be a code. The following hold.

1. $0 \leq \rho(\mathscr{C}) \leq n$. Moreover, $\rho(\mathscr{C}) = 0$ if and only if $\mathscr{C} = \mathbb{F}_q^{n\times m}$.
2. If $\mathscr{D} \subseteq \mathbb{F}_q^{n\times m}$ is a code with $\mathscr{C} \subseteq \mathscr{D}$, then $\rho(\mathscr{C}) \geq \rho(\mathscr{D})$.
3. If $\mathscr{D} \subseteq \mathbb{F}_q^{n\times m}$ is a code with $\mathscr{C} \subsetneq \mathscr{D}$, then $\rho(\mathscr{C}) \geq d(\mathscr{D})$.

First properties of the covering radius

Lemma

Let $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ be a code. The following hold.

1. $0 \leq \rho(\mathscr{C}) \leq n$. Moreover, $\rho(\mathscr{C}) = 0$ if and only if $\mathscr{C} = \mathbb{F}_q^{n\times m}$.
2. If $\mathscr{D} \subseteq \mathbb{F}_q^{n\times m}$ is a code with $\mathscr{C} \subseteq \mathscr{D}$, then $\rho(\mathscr{C}) \geq \rho(\mathscr{D})$.
3. If $\mathscr{D} \subseteq \mathbb{F}_q^{n\times m}$ is a code with $\mathscr{C} \subsetneq \mathscr{D}$, then $\rho(\mathscr{C}) \geq d(\mathscr{D})$.

A code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is **maximal** if $|\mathscr{C}| = 1$ or $|\mathscr{C}| \geq 2$ and there is no code $\mathscr{D} \subseteq \mathbb{F}_q^{n\times m}$ with $\mathscr{D} \supsetneq \mathscr{C}$ and $d(\mathscr{D}) = d(\mathscr{C})$. In particular, $\mathbb{F}_q^{n\times m}$ is maximal.

Proposition

A code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ with $|\mathscr{C}| \geq 2$ is maximal if and only if $\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1$.

Maximality

We introduce a parameter that measures the maximality of a code.

Definition

The **maximality degree** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ with $|\mathscr{C}| \geq 2$ is the integer defined by

$$\mu(\mathscr{C}) := \begin{cases} \min\{d(\mathscr{C}) - d(\mathscr{D}) \mid \mathscr{D} \subseteq \mathbb{F}_q^{n\times m} \text{ is a code with } \mathscr{D} \supsetneq \mathscr{C}\} & \text{if } \mathscr{C} \subsetneq \mathbb{F}_q^{n\times m}, \\ 1 & \text{if } \mathscr{C} = \mathbb{F}_q^{n\times m}. \end{cases}$$

Maximality

We introduce a parameter that measures the maximality of a code.

Definition

The **maximality degree** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ with $|\mathscr{C}| \geq 2$ is the integer defined by

$$\mu(\mathscr{C}) := \begin{cases} \min\{d(\mathscr{C}) - d(\mathscr{D}) \mid \mathscr{D} \subseteq \mathbb{F}_q^{n\times m} \text{ is a code with } \mathscr{D} \supsetneq \mathscr{C}\} & \text{if } \mathscr{C} \subsetneq \mathbb{F}_q^{n\times m}, \\ 1 & \text{if } \mathscr{C} = \mathbb{F}_q^{n\times m}. \end{cases}$$

We have:

- $\mu(\mathscr{C})$ is the "minimum price" (in terms of minimum distance) that one has to pay in order to enlarge $\mathscr{C}$ to a bigger code,
- $0 \leq \mu(\mathscr{C}) \leq d(\mathscr{C}) - 1$,
- $\mu(\mathscr{C}) > 0$ if and only if $\mathscr{C}$ is maximal.

Maximality

We introduce a parameter that measures the maximality of a code.

Definition

The **maximality degree** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ with $|\mathscr{C}| \geq 2$ is the integer defined by

$$\mu(\mathscr{C}) := \begin{cases} \min\{d(\mathscr{C}) - d(\mathscr{D}) \mid \mathscr{D} \subseteq \mathbb{F}_q^{n\times m} \text{ is a code with } \mathscr{D} \supsetneq \mathscr{C}\} & \text{if } \mathscr{C} \subsetneq \mathbb{F}_q^{n\times m}, \\ 1 & \text{if } \mathscr{C} = \mathbb{F}_q^{n\times m}. \end{cases}$$

We have:

- $\mu(\mathscr{C})$ is the "minimum price" (in terms of minimum distance) that one has to pay in order to enlarge $\mathscr{C}$ to a bigger code,
- $0 \leq \mu(\mathscr{C}) \leq d(\mathscr{C}) - 1$,
- $\mu(\mathscr{C}) > 0$ if and only if $\mathscr{C}$ is maximal.

Proposition (Byrne-R.)

For any code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ with $|\mathscr{C}| \geq 2$ we have $\mu(\mathscr{C}) = d(\mathscr{C}) - \min\{\rho(\mathscr{C}),\ d(\mathscr{C})\}$.
In particular, if $\mathscr{C}$ is maximal then $\rho(\mathscr{C}) = d(\mathscr{C}) - \mu(\mathscr{C})$.

Translates of a code

For a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$, let $W_i(\mathscr{C}) := |\{M \in \mathscr{C} \mid \mathrm{rk}(M) = i\}|$.

The **translate** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ by a matrix $X \in \mathbb{F}_q^{n \times m}$ is the code

$$\mathscr{C} + X := \{M + X : M \in \mathscr{C}\} \subseteq \mathbb{F}_q^{n \times m}.$$

Remark

Full knowledge of the weight distribution of the translates of $\mathscr{C}$ tells us the covering radius, as

$$\rho(\mathscr{C}) = \max_{X \in \mathbb{F}_q^{n \times m}} \min_{N \in \mathscr{C} + X} \mathrm{rk}(N).$$

Even partial information may yield a bound on the covering radius.

Translates of a code

For a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$, let $W_i(\mathscr{C}) := |\{M \in \mathscr{C} \mid \mathrm{rk}(M) = i\}|$.

The **translate** of a code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ by a matrix $X \in \mathbb{F}_q^{n \times m}$ is the code

$$\mathscr{C} + X := \{M + X : M \in \mathscr{C}\} \subseteq \mathbb{F}_q^{n \times m}.$$

Remark

Full knowledge of the weight distribution of the translates of $\mathscr{C}$ tells us the covering radius, as

$$\rho(\mathscr{C}) = \max_{X \in \mathbb{F}_q^{n \times m}} \min_{N \in \mathscr{C} + X} \mathrm{rk}(N).$$

Even partial information may yield a bound on the covering radius.

We now express the weight distribution

$$W_0(\mathscr{C} + X), \ldots, W_n(\mathscr{C} + X)$$

of the translate $\mathscr{C} + X$ of a linear code $\mathscr{C} \subsetneq \mathbb{F}_q^{k \times n}$ in terms of

$$W_0(\mathscr{C} + X), \ldots, W_{n-d^\perp}(\mathscr{C} + X), \qquad \text{where } d^\perp = d(\mathscr{C}^\perp).$$

As an application, we obtain an upper bound on the covering radius of a linear code.

Translates of a code

Weight distribution of translates.

Theorem (Byrne-R.)

Let $\mathscr{C} \subsetneq \mathbb{F}_q^{n \times m}$ be a linear code, and let $X \in \mathbb{F}_q^{n \times m}$. Write $d^\perp := d(\mathscr{C}^\perp)$.
Then for all $i \in \{n-d^\perp+1, \dots, n\}$ we have

$$W_i(\mathscr{C}+X) = \sum_{u=0}^{n-d^\perp} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} n-u \\ i-u \end{bmatrix}_q \sum_{j=0}^{u} W_j(\mathscr{C}+X) \begin{bmatrix} u-j \\ n-j \end{bmatrix}_q + \\ + \sum_{u=n-d^\perp+1}^{i} \begin{bmatrix} n \\ u \end{bmatrix}_q \frac{|\mathscr{C}|}{q^{m(k-u)}}.$$

In particular, the distance distribution of the translate $\mathscr{C}+X$ is completely determined by n, m, $|\mathscr{C}|$ and the weights $W_0(\mathscr{C}+X), \dots, W_{n-d^\perp}(\mathscr{C}+X)$.

Translates of a code

Weight distribution of translates.

Theorem (Byrne-R.)

Let $\mathscr{C} \subsetneq \mathbb{F}_q^{n \times m}$ be a linear code, and let $X \in \mathbb{F}_q^{n \times m}$. Write $d^\perp := d(\mathscr{C}^\perp)$.
Then for all $i \in \{n-d^\perp+1, ..., n\}$ we have

$$W_i(\mathscr{C}+X) = \sum_{u=0}^{n-d^\perp} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} n-u \\ i-u \end{bmatrix}_q \sum_{j=0}^{u} W_j(\mathscr{C}+X) \begin{bmatrix} n-j \\ u-j \end{bmatrix}_q + \\ + \sum_{u=n-d^\perp+1}^{i} \begin{bmatrix} n \\ u \end{bmatrix}_q \frac{|\mathscr{C}|}{q^{m(k-u)}}.$$

In particular, the distance distribution of the translate $\mathscr{C}+X$ is completely determined by n, m, $|\mathscr{C}|$ and the weights $W_0(\mathscr{C}+X), ..., W_{n-d^\perp}(\mathscr{C}+X)$.

Let $X \in \mathbb{F}_q^{n \times m} \notin \mathscr{C}$ be arbitrary. Then $W_0(\mathscr{C}+X) = 0$.

Apply the Theorem with $i := n-d^\perp+1$ and obtain:

Translates of a code and dual distance bound

For $X \in \mathbb{F}_q^{n\times m} \notin \mathscr{C}$ arbitrary:

$$W_{n+d^\perp+1}(\mathscr{C}+X) = \sum_{u=1}^{n-d^\perp} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} n-u \\ i-u \end{bmatrix}_q \sum_{j=1}^{u} W_j(\mathscr{C}+X) \begin{bmatrix} n-j \\ u-j \end{bmatrix}_q + \\ + \begin{bmatrix} n \\ n-d^\perp+1 \end{bmatrix}_q |\mathscr{C}|/q^{m(d^\perp-1)}.$$

Translates of a code and dual distance bound

For $X \in \mathbb{F}_q^{n\times m} \notin \mathscr{C}$ arbitrary:

$$W_{n+d^\perp+1}(\mathscr{C}+X) = \sum_{u=1}^{n-d^\perp} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} n-u \\ i-u \end{bmatrix}_q \sum_{j=1}^{u} W_j(\mathscr{C}+X) \begin{bmatrix} n-j \\ u-j \end{bmatrix}_q + \\ + \begin{bmatrix} n \\ n-d^\perp+1 \end{bmatrix}_q |\mathscr{C}|/q^{m(d^\perp-1)}.$$

In particular, $W_1(\mathscr{C}+X),\dots,W_{n-d^\perp+1}(\mathscr{C}+X)$ cannot be all zero!

Since X was arbitrary, this implies the following.

Corollary (dual distance bound, Byrne-R.)

For any linear code $\mathscr{C} \subsetneq \mathbb{F}_q^{n\times m}$ we have $\rho(\mathscr{C}) \le n - d(\mathscr{C}^\perp)+1$.

We have other bounds for linear / non-linear codes.

Initial sets

Let $a, b \in \mathbb{Z}_{>0}$ and $S \subseteq \{1, \ldots, a\} \times \{1, \ldots, b\}$. The **characteristic matrix** $\mathbb{I}(S) \in \mathbb{F}_2^{a \times b}$ of S is defined by

$$\mathbb{I}(S)_{ij} := \begin{cases} 1 & \text{if } (i,j) \in S, \\ 0 & \text{if } (i,j) \notin S \end{cases}$$

Initial sets

Let $a, b \in \mathbb{Z}_{>0}$ and $S \subseteq \{1, \ldots, a\} \times \{1, \ldots, b\}$. The **characteristic matrix** $\mathbb{I}(S) \in \mathbb{F}_2^{a \times b}$ of S is defined by

$$\mathbb{I}(S)_{ij} := \begin{cases} 1 & \text{if } (i,j) \in S, \\ 0 & \text{if } (i,j) \notin S \end{cases}$$

Moreover, we denote by $\lambda(S)$ the minimum number of lines (rows or columns) required to cover all the ones in $\mathbb{I}(S)$.

Example

Let $a = 2,\ b = 3$ and $S = \{(1,1), (1,2), (2,2), (2,3)\}$. Then

$$\mathbb{I}(S) := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{2 \times 3} \qquad \text{and} \qquad \lambda(S) = 2.$$

Initial sets

Let $a, b \in \mathbb{Z}_{>0}$ and $S \subseteq \{1,\dots,a\} \times \{1,\dots,b\}$. The **characteristic matrix** $\mathbb{I}(S) \in \mathbb{F}_2^{a \times b}$ of S is defined by

$$\mathbb{I}(S)_{ij} := \begin{cases} 1 & \text{if } (i,j) \in S, \\ 0 & \text{if } (i,j) \notin S \end{cases}$$

Moreover, we denote by $\lambda(S)$ the minimum number of lines (rows or columns) required to cover all the ones in $\mathbb{I}(S)$.

Example

Let $a = 2,\ b = 3$ and $S = \{(1,1),(1,2),(2,2),(2,3)\}$. Then

$$\mathbb{I}(S) := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{2\times 3} \qquad \text{and} \qquad \lambda(S) = 2.$$

The **initial entry** of a matrix $M \in \mathbb{F}_q^{n \times m}$, $M \neq 0$, is

$$\text{in}(M) := \min\{(i,j) \in \{1,\dots,n\} \times \{1,\dots,m\} \mid M_{ij} \neq 0\} \qquad \text{lexicographically.}$$

Initial sets

Example

Let

$$M := \begin{bmatrix} 0 & 0 & 4 & 2 & 0 \\ 1 & 0 & 3 & 2 & 1 \end{bmatrix} \in \mathbb{F}_5^{2\times 5}$$

Then $\mathrm{in}(M) = (1, 3)$.

Initial sets

Example

Let

$$M := \begin{bmatrix} 0 & 0 & 4 & 2 & 0 \\ 1 & 0 & 3 & 2 & 1 \end{bmatrix} \in \mathbb{F}_5^{2\times 5}$$

Then $\mathrm{in}(M) = (1,3)$.

Definition

The **initial set** of a non-zero linear code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is

$$\mathrm{in}(\mathscr{C}) := \{\mathrm{in}(M) \mid M \in \mathscr{C},\ M \neq 0\} \quad \subseteq \{1,\dots,n\} \times \{1,\dots,m\}.$$

Initial sets

Example

Let

$$M := \begin{bmatrix} 0 & 0 & 4 & 2 & 0 \\ 1 & 0 & 3 & 2 & 1 \end{bmatrix} \in \mathbb{F}_5^{2\times 5}$$

Then $\mathrm{in}(M) = (1,3)$.

Definition

The **initial set** of a non-zero linear code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is

$$\mathrm{in}(\mathscr{C}) := \{\mathrm{in}(M) \mid M \in \mathscr{C},\ M \neq 0\} \quad \subseteq \{1,\dots,n\} \times \{1,\dots,m\}.$$

First properties of the initial set.

Remark

Let $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ be a non-zero linear code. Then

$$\dim(\mathscr{C}) = |\mathrm{in}(\mathscr{C})|.$$

Initial set bound

Theorem (initial set bound, Byrne-R.)

Let $\{0\} \neq \mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ be a linear code. Let $S := \{1, \dots, n - d(\mathscr{C}) + 1\} \times \{1, \dots, m\} \setminus \mathrm{in}(\mathscr{C})$. Then

$$\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1 + \lambda(S).$$

Initial set bound

Theorem (initial set bound, Byrne-R.)

Let $\{0\} \neq \mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ be a linear code. Let $S := \{1,\dots,n-d(\mathscr{C})+1\} \times \{1,\dots,m\} \setminus \mathrm{in}(\mathscr{C})$. Then

$$\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1 + \lambda(S).$$

Example

Let $q = 2$ and $n = m = 3$. Let $\mathscr{C}$ be the linear code generated by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We have $d(\mathscr{C}) = 2$ and $\mathrm{in}(\mathscr{C}) = \{(1,1),(1,2),(2,1),(2,2)\}$.

Initial set bound

Theorem (initial set bound, Byrne-R.)

Let $\{0\} \neq \mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ be a linear code. Let $S := \{1, ..., n - d(\mathscr{C}) + 1\} \times \{1, ..., m\} \setminus \mathrm{in}(\mathscr{C})$. Then

$$\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1 + \lambda(S).$$

Example

Let $q = 2$ and $n = m = 3$. Let $\mathscr{C}$ be the linear code generated by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We have $d(\mathscr{C}) = 2$ and $\mathrm{in}(\mathscr{C}) = \{(1,1),(1,2),(2,1),(2,2)\}$. Therefore

$$S = \{1, ..., 2\} \times \{1, ..., 3\} \setminus \mathrm{in}(\mathscr{C}) = \{(1,3),(2,3)\}, \qquad \mathbb{I}(S) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Initial set bound

Theorem (initial set bound, Byrne-R.)

Let $\{0\} \neq \mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ be a linear code. Let $S := \{1,\dots,n-d(\mathscr{C})+1\} \times \{1,\dots,m\} \setminus \mathrm{in}(\mathscr{C})$. Then

$$\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1 + \lambda(S).$$

Example

Let $q=2$ and $n=m=3$. Let $\mathscr{C}$ be the linear code generated by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We have $d(\mathscr{C}) = 2$ and $\mathrm{in}(\mathscr{C}) = \{(1,1),(1,2),(2,1),(2,2)\}$. Therefore

$$S = \{1,\dots,2\} \times \{1,\dots,3\} \setminus \mathrm{in}(\mathscr{C}) = \{(1,3),(2,3)\}, \qquad \mathbb{I}(S) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

So $\lambda(S) = 1$ and (by the Theorem) $\rho(\mathscr{C}) \leq d(\mathscr{C}) - 1 + \lambda(S) = 2$.

The other bounds give $\rho(\mathscr{C}) \leq 3$.

Other results

If $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ is a linear code of dimension k and $m \gg 0$, then we can say what the "expected" covering radius of $\mathscr{C}$ is for $q \to +\infty$.

Other results

If $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is a linear code of dimension k and $m \gg 0$, then we can say what the "expected" covering radius of $\mathscr{C}$ is for $q \to +\infty$.

Theorem (Byrne-R.)

Let $0 \leq k \leq nm$ be an integer. Denote by $\mathscr{F}$ the family of linear codes $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ of dimension k, and let $\rho_k := n - \lfloor k/m \rfloor$. Let $\mathscr{F}' := \{\mathscr{C} \in \mathscr{F} \mid \rho(\mathscr{C}) = \rho_k\}$. Then

$$\lim_{q\to+\infty} \frac{|\mathscr{F}'|}{|\mathscr{F}|} = 1 \qquad \text{whenever} \qquad k < (m-n+\lfloor k/m \rfloor+1)(\lfloor k/m \rfloor+1).$$

Other results

If $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ is a linear code of dimension k and $m \gg 0$, then we can say what the "expected" covering radius of $\mathscr{C}$ is for $q \to +\infty$.

Theorem (Byrne-R.)

Let $0 \leq k \leq nm$ be an integer. Denote by $\mathscr{F}$ the family of linear codes $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$ of dimension k, and let $\rho_k := n - \lfloor k/m \rfloor$. Let $\mathscr{F}' := \{\mathscr{C} \in \mathscr{F} \mid \rho(\mathscr{C}) = \rho_k\}$. Then

$$\lim_{q\to+\infty} \frac{|\mathscr{F}'|}{|\mathscr{F}|} = 1 \qquad \text{whenever} \qquad k < (m-n+\lfloor k/m \rfloor+1)(\lfloor k/m \rfloor+1).$$

Thank you for your attention!