Reaching singleton bound decoding for Bounded Degree-LRPC codes

Ermes Franch, Chunlei Li

February 12, 2024

University of Bergen, Norway

Summary

Present the bounded degree family of LRPC codes in $\mathbb{F}_{q^m}^n$. Show a probabilistic decoding algorithm for the rate

$$R = 1 - c\rho$$

for large values of m and $1 \leq c < 2$.

Asymptotically

$$n \to \infty, m \to \infty,$$

$$c \to 1, P_{dec} \to 1$$

Summary

Present the bounded degree family of LRPC codes in $\mathbb{F}_{q^m}^n$. Show a probabilistic decoding algorithm for the rate

$$R = 1 - c\rho$$

for large values of m and $1 \leq c < 2$.

Asymptotically

$$n \to \infty, m \to \infty,$$

$$c \to 1, P_{dec} \to 1$$

Summary

Present the bounded degree family of LRPC codes in $\mathbb{F}_{q^m}^n$. Show a probabilistic decoding algorithm for the rate

$$R = 1 - c\rho$$

for large values of m and $1 \leq c < 2$.

Asymptotically

$$n \to \infty, m \to \infty,$$

$$c \to 1, P_{dec} \to 1$$

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Summary

Background Rank metric ($\mathbb{F}_{q^m}$-linear) codes.

LRPC codes and BD-LRPC.

Error support recovery for LRPC.

Expand syndrome space of BD-LRPC.

Matrix representation of the expansion.

Study the "RowSpace expansion" problem.

Rank Support

Let $S = \{s_1, \dots s_N\} \subseteq \mathbb{F}_{q^m}$ the **support** of S is the $\mathbb{F}_q$-subspace generated by the elements of S

$$\langle S \rangle_{\mathbb{F}_q} := \langle s_1, \dots, s_N \rangle_{\mathbb{F}_q}$$

Similarly for $\mathbf{e} = (e_1, \dots, e_n) \in \mathbb{F}_{q^m}^n$

$$\langle \mathbf{e} \rangle_{\mathbb{F}_q} := \langle e_1, \dots, e_n \rangle_{\mathbb{F}_q}.$$

For $H \in \mathbb{F}_{q^m}^{n_1 \times n_2}$

$$\langle H \rangle_{\mathbb{F}_q} := \langle h_{i,j} \mid (i,j) \in [n_1] \times [n_2] \rangle_{\mathbb{F}_q}.$$

Rank Support

Let $S = \{s_1, \dots s_N\} \subseteq \mathbb{F}_{q^m}$ the **support** of S is the $\mathbb{F}_q$-subspace generated by the elements of S

$$\langle S \rangle_{\mathbb{F}_q} := \langle s_1, \dots, s_N \rangle_{\mathbb{F}_q}$$

Similarly for $\mathbf{e} = (e_1, \dots, e_n) \in \mathbb{F}_{q^m}^n$

$$\langle \mathbf{e} \rangle_{\mathbb{F}_q} := \langle e_1, \dots, e_n \rangle_{\mathbb{F}_q}.$$

For $H \in \mathbb{F}_{q^m}^{n_1 \times n_2}$

$$\langle H \rangle_{\mathbb{F}_q} := \langle h_{i,j} \mid (i,j) \in [n_1] \times [n_2] \rangle_{\mathbb{F}_q}.$$

Rank Support

Let $S = \{s_1, \dots s_N\} \subseteq \mathbb{F}_{q^m}$ the **support** of S is the $\mathbb{F}_q$-subspace generated by the elements of S

$$\langle S \rangle_{\mathbb{F}_q} := \langle s_1, \dots, s_N \rangle_{\mathbb{F}_q}$$

Similarly for $\mathbf{e} = (e_1, \dots, e_n) \in \mathbb{F}_{q^m}^n$

$$\langle \mathbf{e} \rangle_{\mathbb{F}_q} := \langle e_1, \dots, e_n \rangle_{\mathbb{F}_q}.$$

For $H \in \mathbb{F}_{q^m}^{n_1 \times n_2}$

$$\langle H \rangle_{\mathbb{F}_q} := \langle h_{i,j} \mid (i,j) \in [n_1] \times [n_2] \rangle_{\mathbb{F}_q}.$$

Rank distance

Given two vectors $\mathbf{v}, \mathbf{u} \in \mathbb{F}_{q^m}^n$ their **rank distance** is defined as:

$$d(\mathbf{v}, \mathbf{u}) = \dim(\langle \mathbf{v} - \mathbf{u} \rangle_{\mathbb{F}_q}).$$

The **rank weight** of $\mathbf{v}$ is defined as:

$$\mathrm{w_R}(\mathbf{v}) = \dim(\langle \mathbf{v} \rangle_{\mathbb{F}_q}).$$

$\mathbb{F}_{q^m}$-linear Rank metric codes

A **rank metric code** is a subset $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$.

An $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is said to be an **$\mathbb{F}_{q^m}$-linear rank metric code**.

It will have a generator $G \in \mathbb{F}_{q^m}^{k \times n}$ and a parity check matrix $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$.

RSD Problem

The Rank Syndrome Decoding (RSD) problem:

RSD Problem
Given H an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$, a vector $\mathbf{s}$ in $\mathbb{F}_{q^m}^{n-k}$ and a small integer r, find a vector $\mathbf{e} \in \mathbb{F}_{q^m}^{n}$ of rank weight $\mathrm{w_R}(\mathbf{e}) \leq r$ such that $\mathbf{e}H^{\intercal} = \mathbf{s}$.

Decoding of $\mathbb{F}_{q^m}$-linear rank metric codes.

An error $\mathbf{e}$ of $\mathrm{w_R}(\mathbf{e}) = r$ can be decomposed as:

$$\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_r)X, \quad X \in \mathbb{F}_q^{r \times n}$$

A good decoding strategy is

- Find a base for the error support $\langle \mathbf{e} \rangle_{\mathbb{F}_q} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{F}_q}$.
- Find the error coordinates X.

Decoding of $\mathbb{F}_{q^m}$-linear rank metric codes.

An error $\mathbf{e}$ of $\mathrm{w_R}(\mathbf{e}) = r$ can be decomposed as:

$$\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_r)X, \quad X \in \mathbb{F}_q^{r \times n}$$

A good decoding strategy is

- Find a base for the error support $\langle \mathbf{e} \rangle_{\mathbb{F}_q} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{F}_q}$.
- Find the error coordinates X.

Decoding of $\mathbb{F}_{q^m}$-linear rank metric codes.

An error $\mathbf{e}$ of $\mathrm{w_R}(\mathbf{e}) = r$ can be decomposed as:

$$\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_r)X, \quad X \in \mathbb{F}_q^{r \times n}$$

A good decoding strategy is

- Find a base for the error support $\langle \mathbf{e} \rangle_{\mathbb{F}_q} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{F}_q}$.
- Find the error coordinates X.

Decoding of $\mathbb{F}_{q^m}$-linear rank metric codes.

An error $\mathbf{e}$ of $\mathrm{w_R}(\mathbf{e}) = r$ can be decomposed as:

$$\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_r)X, \quad X \in \mathbb{F}_q^{r \times n}$$

A good decoding strategy is

- Find a base for the error support $\langle \mathbf{e} \rangle_{\mathbb{F}_q} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{F}_q}$.
- Find the error coordinates X.

LRPC codes

A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is said **LRPC** of density d if it admits a parity check matrix H such that $\dim(\langle H \rangle_{\mathbb{F}_q}) \leq d < m$.

Error support recover

Recover $\mathrm{Supp}(\mathbf{e}) = \mathcal{E}$ from $\mathbf{e}H^{\intercal} = \mathbf{s}$.

$$\mathcal{E} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle, \quad \langle H \rangle = \langle a_1, \ldots, a_d \rangle = \mathcal{A}.$$

Define:

$$\mathcal{E}.\mathcal{A} = \langle (\varepsilon_1, \ldots, \varepsilon_r) \otimes (a_1, \ldots, a_d) \rangle_{\mathbb{F}_q} = \langle \varepsilon_i a_j \rangle_{\mathbb{F}_q}.$$

Key observation

$$\mathbf{s} = \mathbf{e}H^{\intercal} \Rightarrow \langle \mathbf{s} \rangle_{\mathbb{F}_q} \subseteq \mathcal{E}.\mathcal{A}, \qquad \dim(\mathcal{E}.\mathcal{A}) \leq rd.$$

Error support recover

Recover $\mathrm{Supp}(\mathbf{e}) = \mathcal{E}$ from $\mathbf{e}H^\intercal = \mathbf{s}$.

$$\mathcal{E} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle, \quad \langle H \rangle = \langle a_1, \ldots, a_d \rangle = \mathcal{A}.$$

Define:

$$\mathcal{E}.\mathcal{A} = \langle (\varepsilon_1, \ldots, \varepsilon_r) \otimes (a_1, \ldots, a_d) \rangle_{\mathbb{F}_q} = \langle \varepsilon_i a_j \rangle_{\mathbb{F}_q}.$$

Key observation

$$\mathbf{s} = \mathbf{e}H^\intercal \Rightarrow \langle \mathbf{s} \rangle_{\mathbb{F}_q} \subseteq \mathcal{E}.\mathcal{A}, \qquad \dim(\mathcal{E}.\mathcal{A}) \leq rd.$$

Error support recover

Recover $\mathrm{Supp}(\mathbf{e}) = \mathcal{E}$ from $\mathbf{e}H^{\intercal} = \mathbf{s}$.

$$\mathcal{E} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle, \quad \langle H \rangle = \langle a_1, \ldots, a_d \rangle = \mathcal{A}.$$

Define:

$$\mathcal{E}.\mathcal{A} = \langle (\varepsilon_1, \ldots, \varepsilon_r) \otimes (a_1, \ldots, a_d) \rangle_{\mathbb{F}_q} = \langle \varepsilon_i a_j \rangle_{\mathbb{F}_q}.$$

Key observation

$$\mathbf{s} = \mathbf{e}H^{\intercal} \Rightarrow \langle \mathbf{s} \rangle_{\mathbb{F}_q} \subseteq \mathcal{E}.\mathcal{A}, \qquad \dim(\mathcal{E}.\mathcal{A}) \leq rd.$$

From $\mathcal{S}$ to $\mathcal{E}$

In general

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} \subseteq \mathcal{E}.\mathcal{A}.$$

When equality holds

$$\mathcal{S} = a_1\mathcal{E} + \cdots + a_i\mathcal{E} + \cdots + a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

From $\mathcal{S}$ to $\mathcal{E}$

If $n - k \geq rd$, with a good probability

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} = \mathcal{E}.\mathcal{A}.$$

When equality holds

$$\mathcal{S} = a_1\mathcal{E} + \cdots + a_i\mathcal{E} + \cdots + a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

From $\mathcal{S}$ to $\mathcal{E}$

If $n - k \geq rd$, with a good probability

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} = \mathcal{E}.\mathcal{A}.$$

When equality holds

$$\mathcal{S} = a_1\mathcal{E} + \cdots + a_i\mathcal{E} + \cdots + a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

From $\mathcal{S}$ to $\mathcal{E}$

If $n - k \geq rd$, with a good probability

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} = \mathcal{E}.\mathcal{A}.$$

When equality holds

$$a_i^{-1}\mathcal{S} = a_i^{-1}a_1\mathcal{E} + \cdots + \mathcal{E} + \cdots + a_i^{-1}a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

From $\mathcal{S}$ to $\mathcal{E}$

If $n - k \geq rd$, with a good probability

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} = \mathcal{E}.\mathcal{A}.$$

When equality holds

$$a_i^{-1}\mathcal{S} = a_i^{-1}a_1\mathcal{E} + \cdots + \mathcal{E} + \cdots + a_i^{-1}a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

From $\mathcal{S}$ to $\mathcal{E}$

If $n - k \geq rd$, with a good probability

$$\mathcal{S} = \langle \mathbf{s} \rangle_{\mathbb{F}_q} = \mathcal{E}.\mathcal{A}.$$

When equality holds

$$a_i^{-1}\mathcal{S} = a_i^{-1}a_1\mathcal{E} + \cdots + \mathcal{E} + \cdots + a_i^{-1}a_d\mathcal{E}.$$

Since

$$\mathcal{E} \subset a_i^{-1}\mathcal{S}, \qquad \forall i \in \{1, \ldots, d\}.$$

Most likely

$$\mathcal{E} = \bigcap_{i=1}^{d} a_i^{-1}\mathcal{S}.$$

Consequences on achievable Rate

We need $\mathcal{S} = \mathcal{A}.\mathcal{E}$ then

$$n - k \geq \dim(\mathcal{S}) = \dim(\mathcal{A}.\mathcal{E}) \approx dr.$$

Let $R = k/n$ and $\rho = r/n$.

$$R \leq 1 - d\rho,$$

where $d \geq 2$

Consequences on achievable Rate

We need $\mathcal{S} = \mathcal{A}.\mathcal{E}$ then

$$n - k \geq \dim(\mathcal{S}) = \dim(\mathcal{A}.\mathcal{E}) \approx dr.$$

Let $R = k/n$ and $\rho = r/n$.

$$R \leq 1 - d\rho,$$

where $d \geq 2$.

Similar work

In [1] Aragon, Gaborit, Hauteville, Ruatta and Zémor. For LRPC of density $d = 2$

$$R \leq 1 - \frac{3}{2}\rho,$$

For Bounded Degree LRPC

$$R \leq 1 - c\rho,$$

where $1 \leq c < 2$ and $c \to 1$ for $m \to \infty$.

Similar work

In [1] Aragon, Gaborit, Hauteville, Ruatta and Zémor. For LRPC of density $d = 2$

$$R \leq 1 - \frac{3}{2}\rho,$$

For Bounded Degree LRPC

$$R \leq 1 - c\rho,$$

where $1 \leq c < 2$ and $c \to 1$ for $m \to \infty$.

Bounded degree LRPC codes

Bounded degree LRPC codes
A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is said Bounded degree **LRPC** of bounded degree d if it admits a parity check matrix H such that $\langle H \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,d}$ where $\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \dots \alpha^{d-1} \rangle_{\mathbb{F}_q}$.

LRPC of density $d = 2$

$$\langle H \rangle_{\mathbb{F}_q} = \langle a_1, a_2 \rangle_{\mathbb{F}_q}.$$

Bounded degree LRPC of bounded degree $d = 2$.

$$\langle a_1^{-1} H \rangle_{\mathbb{F}_q} = \langle 1, \alpha \rangle_{\mathbb{F}_q}, \quad \alpha = a_1^{-1} a_2.$$

Bounded degree LRPC codes
A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is said Bounded degree **LRPC** of bounded degree d if it admits a parity check matrix H such that $\langle H \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,d}$ where $\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \dots \alpha^{d-1} \rangle_{\mathbb{F}_q}$.

LRPC of density $d = 2$

$$\langle H \rangle_{\mathbb{F}_q} = \langle a_1, a_2 \rangle_{\mathbb{F}_q}.$$

Bounded degree LRPC of bounded degree $d = 2$.

$$\langle a_1^{-1} H \rangle_{\mathbb{F}_q} = \langle 1, \alpha \rangle_{\mathbb{F}_q}, \quad \alpha = a_1^{-1} a_2.$$

Bounded degree LRPC codes
A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is said Bounded degree **LRPC** of bounded degree d if it admits a parity check matrix H such that $\langle H \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,d}$ where $\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \dots \alpha^{d-1} \rangle_{\mathbb{F}_q}$.

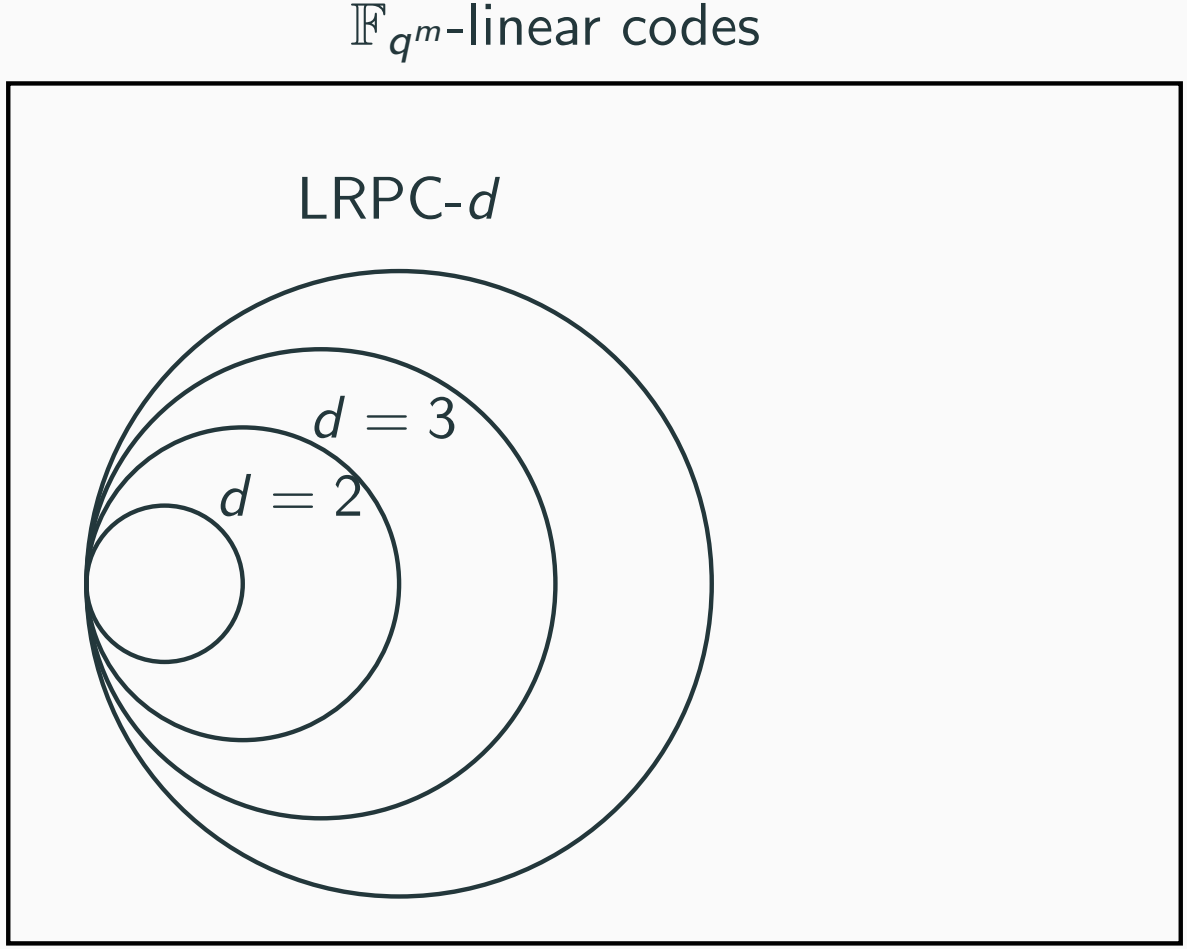
LRPC of density $d = 2$

$$\langle H \rangle_{\mathbb{F}_q} = \langle a_1, a_2 \rangle_{\mathbb{F}_q}.$$

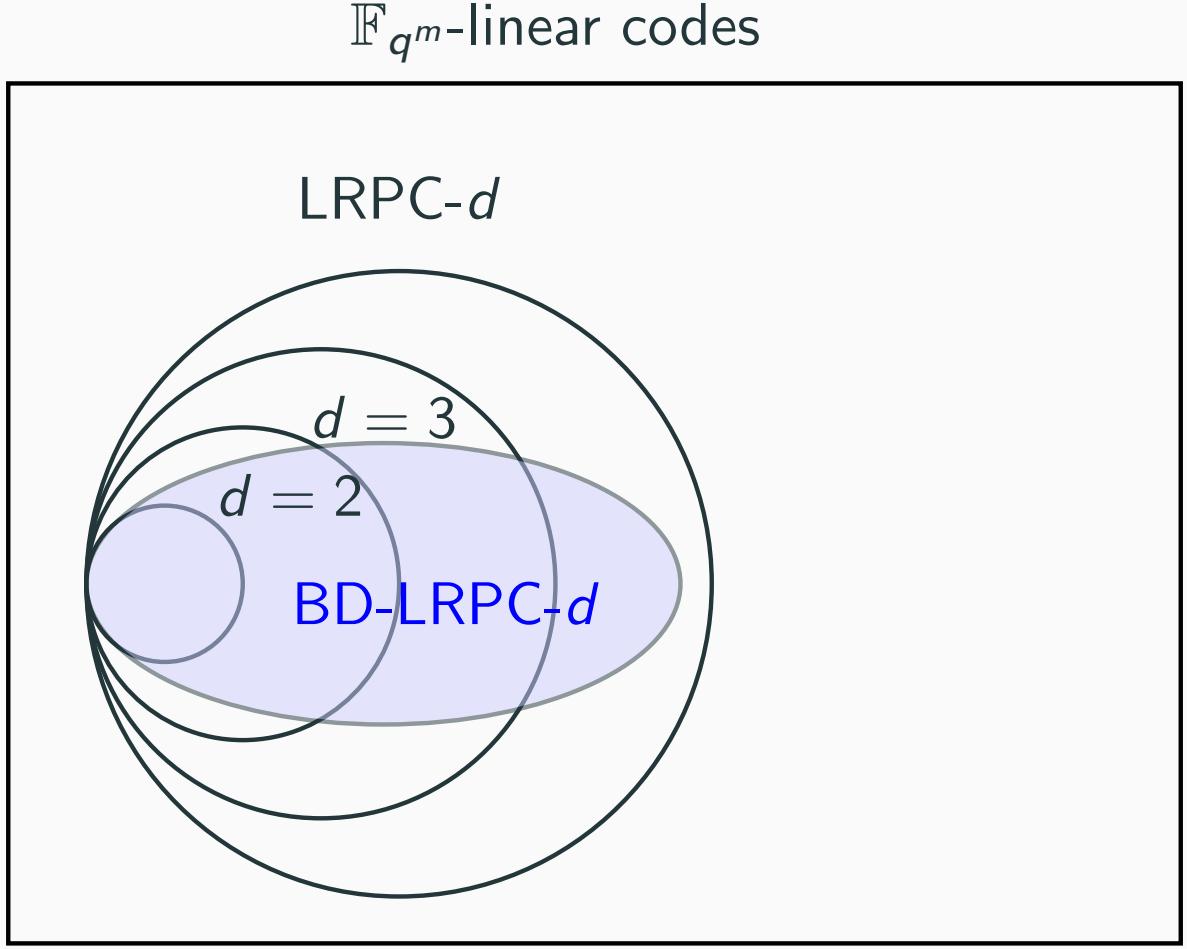
Bounded degree LRPC of bounded degree $d = 2$.

$$\langle a_1^{-1} H \rangle_{\mathbb{F}_q} = \langle 1, \alpha \rangle_{\mathbb{F}_q}, \quad \alpha = a_1^{-1} a_2.$$

BD-LRPC codes inside LRPC codes



BD-LRPC codes inside LRPC codes



Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{S} \subsetneq \mathcal{V}_{\alpha,d}.\mathcal{E}$$

Let $n - k = r + u$

$$t(r + u) \geq (t + d - 1)r$$

Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{S} \subsetneq \mathcal{V}_{\alpha,d}.\mathcal{E}$$

Let $n - k = r + u$

$$t(r+u) \geq (t+d-1)r$$

Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{V}_{\alpha,t}.\mathcal{S} \subseteq \mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d}.\mathcal{E}$$

Let $n - k = r + u$

$$t(r + u) \geq (t + d - 1)r$$

Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{V}_{\alpha,t}.\mathcal{S} \subseteq \mathcal{V}_{\alpha,t+d-1}.\mathcal{E}$$

Let $n - k = r + u$

$$t(r+u) \geq (t+d-1)r$$

Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{V}_{\alpha,t}.\mathcal{S} \subseteq \mathcal{V}_{\alpha,t+d-1}.\mathcal{E}$$

Let $n - k = r + u$

$$t(r + u) \geq (t + d - 1)r$$

Syndrome support expansion

Notice

$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

$$\mathcal{V}_{\alpha,t}.\mathcal{S} \subseteq \mathcal{V}_{\alpha,t+d-1}.\mathcal{E}$$

Let $n - k = r + u$

$$tu \geq (d-1)r$$

Syndrome support expansion

Notice

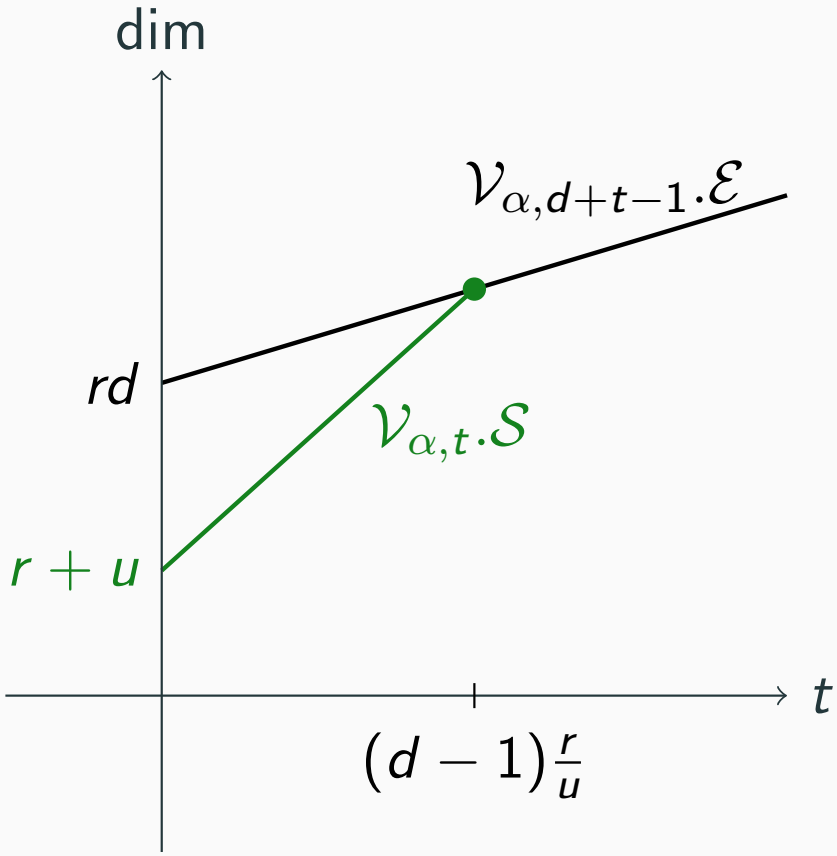
$$\mathcal{V}_{\alpha,t}.\mathcal{V}_{\alpha,d} = \langle 1, \alpha, \ldots, \alpha^{t+d-2} \rangle_{\mathbb{F}_q} = \mathcal{V}_{\alpha,t+d-1}.$$

Suppose

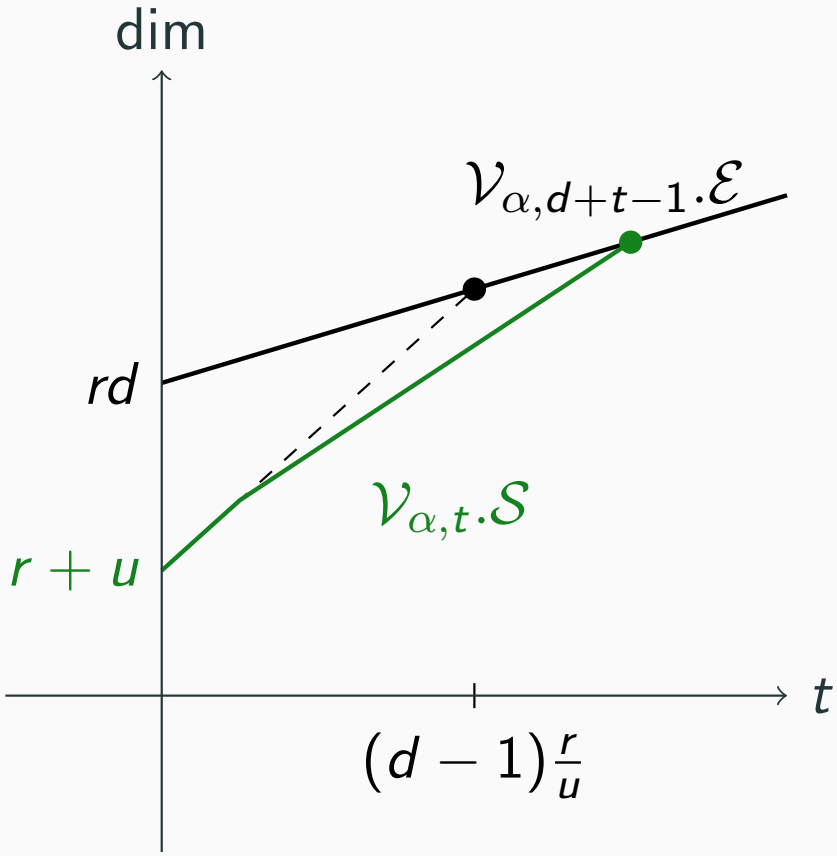
$$\mathcal{V}_{\alpha,t}.\mathcal{S} \subseteq \mathcal{V}_{\alpha,t+d-1}.\mathcal{E}$$

Let $n - k = r + u$

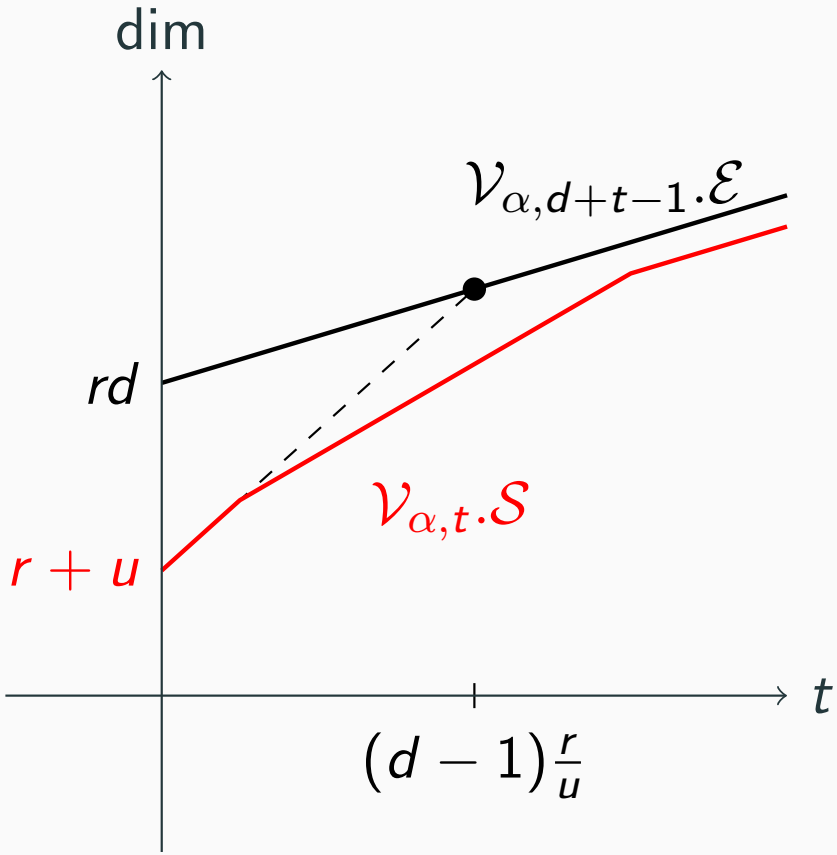
$$t \geq (d-1)\frac{r}{u}.$$



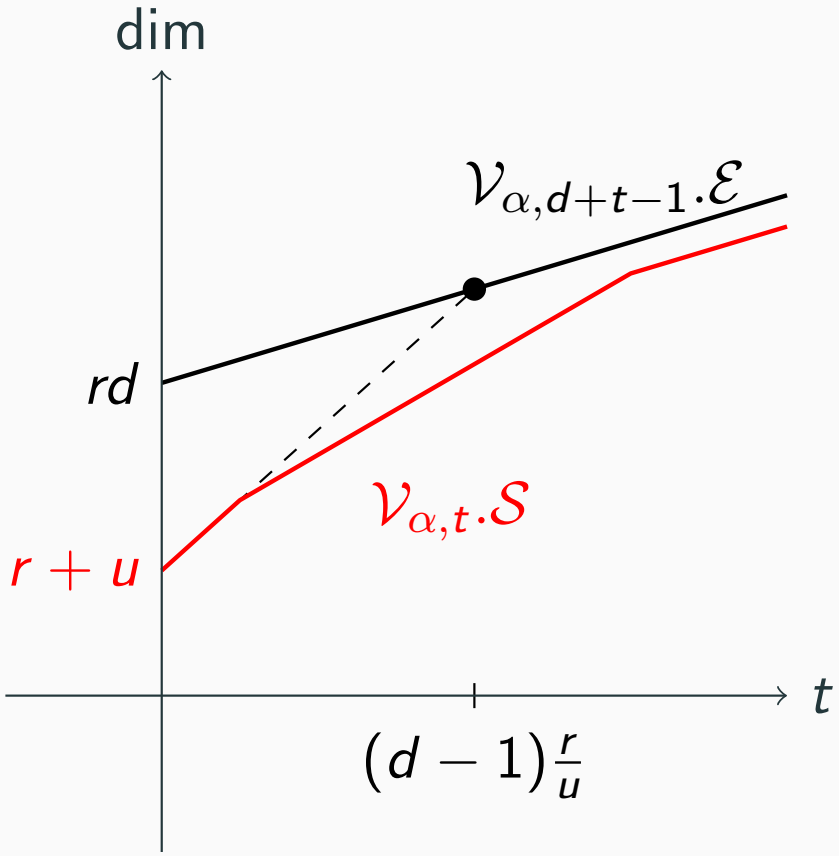
For large $u = (n-k) - r$, convergence is both faster and more likely.



For large $u = (n-k) - r$, convergence is both faster and more likely.



For large $u = (n-k) - r$, convergence is both faster and more likely.



For large $u = (n-k) - r$, convergence is both faster and more likely.

Consequence on achievable Rate

From $n - k = r + u$ we have

$$R \leq 1 - \rho - \mu$$

where

$$\rho = \frac{r}{n}, \quad \mu = \frac{u}{n}.$$

A matrix model

Notice $\mathbf{s} \in \mathcal{V}_{\alpha,d}.\mathcal{E}$ of basis $\mathbf{a}_d \otimes \boldsymbol{\varepsilon}$, where $\mathbf{a}_d = (1, \alpha, \ldots, \alpha^{d-1})$.

$$\begin{pmatrix} s_1 \\ \vdots \\ s_{n-k} \end{pmatrix} = X_1\boldsymbol{\varepsilon}^\intercal + \alpha X_2\boldsymbol{\varepsilon}^\intercal + \ldots + \alpha^{d-1}X_d\boldsymbol{\varepsilon}^\intercal.$$

Where

$$X_i \in \mathbb{F}_q^{(n-k)\times r}$$

A matrix model

Notice $\mathbf{s} \in \mathcal{V}_{\alpha,d}.\mathcal{E}$ of basis $\mathbf{a}_d \otimes \varepsilon$, where $\mathbf{a}_d = (1, \alpha, \ldots, \alpha^{d-1})$.

$$\begin{pmatrix} s_1 \\ \vdots \\ s_{n-k} \end{pmatrix} = (X_1, \ldots, X_d)(\mathbf{a}_d \otimes \varepsilon)^\intercal.$$

Where

$$X_i \in \mathbb{F}_q^{(n-k)\times r}$$

A matrix model

Notice $\mathbf{s} \in \mathcal{V}_{\alpha,d}.\mathcal{E}$ of basis $\mathbf{a}_d \otimes \varepsilon$, where $\mathbf{a}_d = (1, \alpha, \ldots, \alpha^{d-1})$.

$$\alpha \begin{pmatrix} s_1 \\ \vdots \\ s_{n-k} \end{pmatrix} = (\mathbf{0}, X_1, \ldots, X_d)(\mathbf{a}_{d+1} \otimes \varepsilon)^\intercal.$$

Where

$$X_i \in \mathbb{F}_q^{(n-k)\times r}$$

A matrix model

$$\begin{pmatrix} \mathbf{s}^\mathsf{T} \\ \alpha \mathbf{s}^\mathsf{T} \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \dots & X_d & \mathbf{0} \\ \mathbf{0} & X_1 & X_2 & \dots & X_d \end{pmatrix} (\mathbf{a}_{d+1} \otimes \boldsymbol{\varepsilon})^\mathsf{T}.$$

A matrix model

$$\begin{pmatrix} \mathbf{s}^\mathsf{T} \\ \alpha\mathbf{s}^\mathsf{T} \\ \vdots \\ \alpha^{t-1}\mathbf{s}^\mathsf{T} \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \cdots & X_d & 0 & \cdots & 0 \\ 0 & X_1 & X_2 & \cdots & X_d & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & \cdots & 0 & X_1 & X_2 & \cdots & X_d \end{pmatrix} \begin{pmatrix} \boldsymbol{\varepsilon}^\mathsf{T} \\ \alpha\boldsymbol{\varepsilon}^\mathsf{T} \\ \vdots \\ \alpha^{d+t-2}\boldsymbol{\varepsilon}^\mathsf{T} \end{pmatrix}.$$

$\mathcal{V}_{\alpha,t}.\mathcal{S}$ Is this matrix full rank $(d+t-1)r$? $\mathcal{V}_{\alpha,d+t-1}.\mathcal{E}$

A matrix model

$$\begin{pmatrix} \mathbf{s}^\mathsf{T} \\ \alpha\mathbf{s}^\mathsf{T} \\ \vdots \\ \alpha^{t-1}\mathbf{s}^\mathsf{T} \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \cdots & X_d & 0 & \cdots & 0 \\ 0 & X_1 & X_2 & \cdots & X_d & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & \cdots & 0 & X_1 & X_2 & \cdots & X_d \end{pmatrix} \begin{pmatrix} \boldsymbol{\varepsilon}^\mathsf{T} \\ \alpha\boldsymbol{\varepsilon}^\mathsf{T} \\ \vdots \\ \alpha^{d+t-2}\boldsymbol{\varepsilon}^\mathsf{T} \end{pmatrix}.$$

$\downarrow$ $\qquad$ $\downarrow$ $\qquad$ $\downarrow$

$\mathcal{V}_{\alpha,t}.\mathcal{S}$ $\qquad$ Is this matrix full rank $(d+t-1)r$? $\qquad$ $\mathcal{V}_{\alpha,d+t-1}.\mathcal{E}$

A matrix model

$$\begin{pmatrix} \mathbf{s}^\mathsf{T} \\ \alpha\mathbf{s}^\mathsf{T} \\ \vdots \\ \alpha^{t-1}\mathbf{s}^\mathsf{T} \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \cdots & X_d & 0 & \cdots & 0 \\ 0 & X_1 & X_2 & \cdots & X_d & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & \cdots & 0 & X_1 & X_2 & \cdots & X_d \end{pmatrix} \begin{pmatrix} \boldsymbol{\varepsilon}^\mathsf{T} \\ \alpha\boldsymbol{\varepsilon}^\mathsf{T} \\ \vdots \\ \alpha^{d+t-2}\boldsymbol{\varepsilon}^\mathsf{T} \end{pmatrix}.$$

$\mathcal{V}_{\alpha,t}.\mathcal{S}$ — Is this matrix full rank $(d+t-1)r$? — $\mathcal{V}_{\alpha,d+t-1}.\mathcal{E}$

When is this full rank? (d=2)

$$M_t = \begin{pmatrix} X_1 & X_2 & 0 & \cdots & 0 \\ 0 & X_1 & X_2 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & X_1 & X_2 \end{pmatrix}$$

Observe X_1 must be invertible.

When is this full rank? (d=2)

$$PM_t = \begin{pmatrix} Y_1 & Y_2 & & & \\ & Y_1 & Y_2 & & \\ & & \ddots & \ddots & \\ & & & Y_1 & Y_2 \\ Z_1 & Z_2 & & & \\ & Z_1 & Z_2 & & \\ & & \ddots & \ddots & \\ & & & Z_1 & Z_2 \end{pmatrix},$$

where $Y_i \in \mathbb{F}_q^{r \times r}, Z_i \in \mathbb{F}_q^{u \times r}$ and Y_1 is full rank.

When is this full rank? (d=2)

Let A such that $Y_1 A = -Y_2$.

$$M_t = \begin{pmatrix} Y_1 & Y_2 & & & \\ & Y_1 & Y_2 & & \\ & & \ddots & \ddots & \\ & & & Y_1 & Y_2 \\ Z_1 & Z_2 & & & \\ & Z_1 & Z_2 & & \\ & & \ddots & \ddots & \\ & & & Z_1 & Z_2 \end{pmatrix},$$

where $Z = Z_1 A + Z_2$.

When is this full rank? (d=2)

Let A such that $Y_1 A = -Y_2$.

$$M_t = \begin{pmatrix} Y_1 & & & & \\ & Y_1 & Y_2 & & \\ & & \ddots & \ddots & \\ & & & Y_1 & Y_2 \\ Z_1 & Z & & & \\ & Z_1 & Z_2 & & \\ & & \ddots & \ddots & \\ & & & Z_1 & Z_2 \end{pmatrix},$$

where $Z = Z_1 A + Z_2$.

When is this full rank? (d=2)

Let A such that $Y_1 A = -Y_2$.

$$M_t^{(1)} = \begin{pmatrix} Y_1 & & & & \\ & Y_1 & Y_2 & & \\ & & \ddots & \ddots & \\ & & & Y_1 & Y_2 \\ & Z & & & \\ & Z_1 & Z_2 & & \\ & & \ddots & \ddots & \\ & & & Z_1 & Z_2 \end{pmatrix},$$

where $Z = Z_1 A + Z_2$.

When is this full rank? (d=2)

Let A such that $Y_1 A = -Y_2$.

$$M_t^{(2)} = \begin{pmatrix} Y_1 & & & & \\ & Y_1 & & & \\ & & \ddots & \ddots & \\ & & & Y_1 & Y_2 \\ & & ZA & & \\ & & Z & & \\ & & \ddots & \ddots & \\ & & & Z_1 & Z_2 \end{pmatrix},$$

where $Z = Z_1 A + Z_2$.

When is this full rank? (d=2)

Let A such that $Y_1 A = -Y_2$.

$$M_t^{(t)} = \begin{pmatrix} Y_1 & & & & \\ & Y_1 & & & \\ & & \ddots & & \\ & & & Y_1 & \\ & & & & ZA^{t-1} \\ & & & & ZA^{t-2} \\ & & & & \vdots \\ & & & & Z \end{pmatrix}$$

where $Z = Z_1 A + Z_2$.

When is this full rank? (d=2)

$$\text{Rank}(M_t) = r(d+t-1) \iff \text{Rank}(Y_1) = r, \text{Rank}(\tilde{Z}) = r.$$

where

$$\tilde{Z} = \begin{pmatrix} Z \\ ZA \\ \vdots \\ ZA^{t-1} \end{pmatrix} \in \mathbb{F}_q^{ut \times r(d-1)}.$$

When is this full rank? ($d = 2$)

$$\text{Rank}(Y_1) = r \iff \text{Rank}(X_1) = r$$
$$\text{Rank}(\tilde{Z}) = r \iff ?$$

Hypothesis: $X_1, X_2 \in \mathbb{F}_q^{(r+u)\times r}$ are random uniform.

$$P(\text{Rank}(X_1) = r) \approx 1 - \frac{q^{-u}}{(q-1)}$$
$$P(\text{Rank}(\tilde{Z}) = r) \approx 1 - \frac{q^{-u+1}}{q-1}.$$

Matrix expansion

Problem

Let

$$\Omega_t(Z, A) = \mathrm{RowSpan}(Z) + \mathrm{RowSpan}(ZA) + \cdots + \mathrm{RowSpan}(ZA^t),$$

and

$$C_k^{(u,r,t)} = \left\{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} \mid \dim(\Omega_t(Z, A)) = k\right\}.$$

Determine $|C_k^{(u,r,t)}|$.

Basic properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Then

$$\Omega_0(Z, A) \subseteq \Omega_1(Z, A) \subseteq \ldots \subseteq \Omega(Z, A).$$

It can be proved that

$$\Omega(Z, A) = \Omega_{r-1}(Z, A).$$

Basic properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Then

$$\Omega_0(Z, A) \subseteq \Omega_1(Z, A) \subseteq \ldots \subseteq \Omega(Z, A).$$

It can be proved that

$$\Omega(Z, A) = \Omega_{r-1}(Z, A).$$

Basic properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Then

$$\Omega_0(Z, A) \subseteq \Omega_1(Z, A) \subseteq \ldots \subseteq \Omega(Z, A).$$

It can be proved that

$$\Omega(Z, A) = \Omega_{r-1}(Z, A).$$

Basic properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Then

$$\Omega_0(Z, A) \subseteq \Omega_1(Z, A) \subseteq \ldots \subseteq \Omega(Z, A).$$

It can be proved that

$$\Omega(Z, A) = \Omega_{r-1}(Z, A).$$

Generation of a basis for $\Omega_t(Z, A)$

Algorithm 1: Generation of a basis of $\Omega_t(Z, A)$ for $(Z, A), t$

Input: A matrix $Z \in \mathbb{F}_q^{u \times r}$, a matrix $A \in \mathbb{F}_q^{r \times r}$ and an integer t

Output: A matrix G such that $\text{RowSpan}(G) = \Omega_t(Z, A)$.

// Initialize Ω as the zero subspace and G as an empty list.

1 $\Omega = \{\mathbf{0}\}$;

2 $G = []$;

3 **for** $j \in [0 \dots t]$ **do**

  // Add all the new linearly independent rows obtained from ZA^j using the convention $A^0 = I_r$.

4 $G^{(j)} = []$;

5 **for** $i \in [u]$ **do**

6 **if** $\mathbf{z}_i A^j \notin \Omega$ **then**

7 $G^{(j)}.append(\mathbf{z}_i A^j)$;

8 $\Omega = \text{RowSpan}(G) + \langle \mathbf{z}_i A^j \rangle_{\mathbb{F}_q}$;

9 **end**

10 **end**

11 $G.append(G^{(j)})$;

12 **end**

13 Return G;

A running example

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

A running example

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

$$ZI = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \rightarrow G = \left(G^{(0)}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

A running example

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

$$G^{(0)}A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \rightarrow G = \left(\begin{array}{c} G^{(0)} \\ \hline G^{(1)} \end{array}\right) = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \end{array}\right).$$

A running example

$$Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

$$G^{(1)}A = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow G = \left(\begin{array}{c} G^{(0)} \\ \hline G^{(1)} \\ \hline G^{(2)} \end{array}\right) = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Change of basis invariance

Let $B \in GL_r(\mathbb{F}_q)$, since

$$ZB(B^{-1}AB)^j = (ZA^j)B$$

then

$$\Omega_t(ZB, B^{-1}AB) = \Omega_t(Z, A)B$$

and

$$(Z, A) \in C_k^{(u,r,t)} \iff (ZB, B^{-1}AB) \in C_k^{(u,r,t)}$$

Change of basis invariance

Let $B \in GL_r(\mathbb{F}_q)$, since

$$ZB(B^{-1}AB)^j = (ZA^j)B$$

then

$$\Omega_t(ZB, B^{-1}AB) = \Omega_t(Z, A)B$$

and

$$(Z, A) \in C_k^{(u,r,t)} \iff (ZB, B^{-1}AB) \in C_k^{(u,r,t)}$$

Change of basis invariance

Let $B \in GL_r(\mathbb{F}_q)$, since

$$ZB(B^{-1}AB)^j = (ZA^j)B$$

then

$$\Omega_t(ZB, B^{-1}AB) = \Omega_t(Z, A)B$$

and

$$(Z, A) \in C_k^{(u,r,t)} \iff (ZB, B^{-1}AB) \in C_k^{(u,r,t)}$$

How to count $|C_G^{(u,r,t)}|$

Proposition 3

$$C_G^{(u,r,t)} = \{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} : Alg(Z, A, t) = G\},$$

Then:

$$|C_G^{(u,r,t)}| = |C_{E_k}^{(u,r,t)}|.$$

Where

$$E_k = \left(I_k \;\middle|\; \mathbf{0}\right)$$

Key fact:

If $GB = E_k$, then

$$(Z, A) \in C_G^{(u,r,t)} \iff (ZB, B^{-1}AB) \in C_{E_k}^{(u,r,t)}$$

How to count $|C_G^{(u,r,t)}|$

Proposition 3

$$C_G^{(u,r,t)} = \{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} : Alg(Z, A, t) = G\},$$

Then:

$$|C_G^{(u,r,t)}| = |C_{E_k}^{(u,r,t)}|.$$

Where

$$E_k = \left(I_k \;\middle|\; \mathbf{0}\right)$$

Key fact:

If $GB = E_k$, then

$$(Z, A) \in C_G^{(u,r,t)} \iff (ZB, B^{-1}AB) \in C_{E_k}^{(u,r,t)}$$

How to count $|C_k^{(u,r,t)}|$

Corollary 1

$$C_k^{(u,r,t)} = \{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} : Alg(Z, A, t) = G, \mathrm{Rank}(G) = k\}.$$

Then we have

$$|C_k^{(u,r,t)}| = |G||C_{E_k}^{(u,r,t)}| = A_q(r, k)|C_{E_k}^{(u,r,t)}|.$$

Where

$$A_q(r, k) = \prod_{i=0}^{k-1}(q^r - q^i).$$

Matrices $\mathbb{F}_q^{k\times r}$ of rank k.

How to count $|C_k^{(u,r,t)}|$

Corollary 1

$$C_k^{(u,r,t)} = \{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} : Alg(Z, A, t) = G, \mathrm{Rank}(G) = k\}.$$

Then we have

$$|C_k^{(u,r,t)}| = |G||C_{E_k}^{(u,r,t)}| = A_q(r, k)|C_{E_k}^{(u,r,t)}|.$$

Where

$$A_q(r, k) = \prod_{i=0}^{k-1}(q^r - q^i).$$

Matrices $\mathbb{F}_q^{k\times r}$ of rank k.

Counting $|C_{E_k}^{(u,r)}|$

Proposition 4

$$C_{E_k}^{(u,r)} = \left\{(Z, A) \in \mathbb{F}_q^{u\times r} \times \mathbb{F}_q^{r\times r} \mid Alg(Z, A, r-1) = E_k\right\},$$

$$|C_{E_k}^{(u,r)}| = \begin{bmatrix} k+u-1 \\ u-1 \end{bmatrix}_q q^{r(r-k)+k}.$$

Sketch Proof

Observe:

$\mathbf{z}_i \in \text{RowSpan}(E_k)$, so $Z = (\hat{Z}|\mathbf{0})$.

Moreover:

$$\mathbf{v} \in \text{RowSpan}(E_k) \Rightarrow \mathbf{v}A \in \text{RowSpan}(E_k).$$

Then:

$$\left(\begin{array}{c} Z \\ A \end{array}\right) = \left(\begin{array}{c|c} \hat{Z} & \mathbf{0} \\ Y & \\ \hline \multicolumn{2}{c}{\hat{A}} \end{array}\right)$$

There are $q^{(r-k)r}$ choices of $\hat{A} \in \mathbb{F}_q^{(r-k)\times r}$.

Sketch Proof

Observe:

$\mathbf{z}_i \in \text{RowSpan}(E_k)$, so $Z = (\hat{Z}|\mathbf{0})$.

Moreover:

$$\mathbf{v} \in \text{RowSpan}(E_k) \Rightarrow \mathbf{v}A \in \text{RowSpan}(E_k).$$

Then:

$$\begin{pmatrix} Z \\ A \end{pmatrix} = \left(\begin{array}{c|c} \hat{Z} & \mathbf{0} \\ Y & \\ \hline \multicolumn{2}{c}{\hat{A}} \end{array}\right)$$

There are $q^{(r-k)r}$ choices of $\hat{A} \in \mathbb{F}_q^{(r-k)\times r}$.

Sketch Proof

Observe:

$\mathbf{z}_i \in \text{RowSpan}(E_k)$, so $Z = (\hat{Z}|\mathbf{0})$.

Moreover:

$$\mathbf{v} \in \text{RowSpan}(E_k) \Rightarrow \mathbf{v}A \in \text{RowSpan}(E_k).$$

Then:

$$\begin{pmatrix} Z \\ A \end{pmatrix} = \left(\begin{array}{c|c} \hat{Z} & \mathbf{0} \\ Y & \\ \hline \multicolumn{2}{c}{\hat{A}} \end{array}\right)$$

There are $q^{(r-k)r}$ choices of $\hat{A} \in \mathbb{F}_q^{(r-k)\times r}$.

Sketch Proof

Observe:

$\mathbf{z}_i \in \text{RowSpan}(E_k)$, so $Z = (\hat{Z}|\mathbf{0})$.

Moreover:

$$\mathbf{v} \in \text{RowSpan}(E_k) \Rightarrow \mathbf{v}A \in \text{RowSpan}(E_k).$$

Then:

$$\begin{pmatrix} Z \\ A \end{pmatrix} = \left(\begin{array}{c|c} \hat{Z} & \mathbf{0} \\ Y & \\ \hline \multicolumn{2}{c}{\hat{A}} \end{array}\right)$$

There are $q^{(r-k)r}$ choices of $\hat{A} \in \mathbb{F}_q^{(r-k)\times r}$.

Sketch Proof

$$\left(\frac{Z}{A}\right) = \begin{pmatrix} 1000 \\ \bullet 000 \\ 0100 \\ \bullet\bullet 00 \\ \hline 0010 \\ \bullet\bullet\bullet 0 \\ \hline 0001 \\ \hline \bullet\bullet\bullet\bullet \end{pmatrix} = \begin{pmatrix} Z^{(0)} \\ \hline Z^{(1)} \\ \hline Z^{(2)} \\ \hline Z^{(3)} \end{pmatrix} \Longrightarrow E_4 = \begin{pmatrix} G^{(0)} \\ \hline G^{(1)} \\ \hline G^{(2)} \\ \hline G^{(3)} \end{pmatrix} = \begin{pmatrix} 1000 \\ 0100 \\ \hline 0010 \\ \hline 0001 \end{pmatrix}$$

Last row $\mathbf{y}_k$ always q^k possible choices.

Sketch Proof

$$\left(\frac{Z}{A}\right) = \left(\begin{array}{c} 1000 \\ \bullet 000 \\ 0100 \\ \bullet\bullet 00 \\ \hline 0010 \\ \bullet\bullet\bullet 0 \\ \hline 0001 \\ \hline \bullet\bullet\bullet\bullet \end{array}\right) = \left(\begin{array}{c} Z^{(0)} \\ \hline Z^{(1)} \\ \hline Z^{(2)} \\ \hline Z^{(3)} \end{array}\right) \Longrightarrow E_4 = \left(\begin{array}{c} G^{(0)} \\ \hline G^{(1)} \\ \hline G^{(2)} \\ \hline G^{(3)} \end{array}\right) = \left(\begin{array}{c} 1000 \\ 0100 \\ \hline 0010 \\ \hline 0001 \end{array}\right)$$

Last row $\mathbf{y}_k$ always q^k possible choices.

Sketch Proof

The remaining part form a Ferrer's diagram.

$$F = \begin{pmatrix} \bullet 000 \\ \bullet\bullet 00 \\ \bullet\bullet\bullet 0 \end{pmatrix} \in \mathcal{F}_{u-1,k}.$$

Summing all the possible F

$$\sum_{F \in \mathcal{F}_{u-1,k}} q^{|F|} = \begin{bmatrix} k+u-1 \\ u-1 \end{bmatrix}_q.$$

Sketch Proof

The remaining part form a Ferrer's diagram.

$$F = \begin{pmatrix} \bullet 000 \\ \bullet\bullet 00 \\ \bullet\bullet\bullet 0 \end{pmatrix} \in \mathcal{F}_{u-1,k}.$$

Summing all the possible F

$$\sum_{F \in \mathcal{F}_{u-1,k}} q^{|F|} = \begin{bmatrix} k+u-1 \\ u-1 \end{bmatrix}_q.$$

Sketch Proof

$$|C_{E_k}^{(u,r)}| = |\mathcal{F}_{u-1,k}||\hat{A}||\mathbf{y}_k|$$

Sketch Proof

$$|C_{E_k}^{(u,r)}| = \begin{bmatrix} k+u-1 \\ u-1 \end{bmatrix}_q q^{r(r-k)+k}.$$

Finally $|C_k^{(u,r)}|$

Recall Corollary 1:

$$|C_k^{(u,r)}| = A_q(r,k)|C_{E_k}^{(u,r,t)}|.$$

Finally $|C_k^{(u,r)}|$

Recall Corollary 1:

$$|C_k^{(u,r)}| = A_q(r,k) \begin{bmatrix} k+u-1 \\ u-1 \end{bmatrix}_q q^{r(r-k)+k}.$$

Full rank of $\binom{Z}{A}$

Corollary 2

The probability that a random matrix $Y = \begin{pmatrix} Z \\ A \end{pmatrix}$ uniformly drawn from $\mathbb{F}_q^{(r+u)\times r}$ produces a r-dimensional subspace $\Omega(Z, A)$ is

$$\frac{|C_r^{(u,r)}|}{q^{r(r+u)}} \approx 1 - \frac{q^{-u+1}}{q-1}.$$

Conclusion

We show that

$$\mathcal{V}_{\alpha,t}.\mathcal{S} = \mathcal{V}_{\alpha,d+t-1}.\mathcal{E}$$

with a probability in the order of $1 - q^{-u+1}$.

Recall

$$R \leq 1 - \rho - \mu$$

We can fix u while $n \to \infty$. Asymptotically $\mu = \frac{u}{n} \to 0$.

Conclusion

We show that

$$\mathcal{V}_{\alpha,t}.\mathcal{S} = \mathcal{V}_{\alpha,d+t-1}.\mathcal{E}$$

with a probability in the order of $1 - q^{-u+1}$.

Recall

$$R \leq 1 - \rho$$

We can fix u while $n \to \infty$. Asymptotically $\mu = \frac{u}{n} \to 0$.

Requirement on m

$$\mathcal{E} \subseteq \mathcal{V}_{d+t-1}.\mathcal{E} \cap \alpha^{-(d+t-1)}\mathcal{V}_{d+t-1}.\mathcal{E}$$
$$\mathcal{A} \quad \cap \quad \mathcal{B}$$

For equality we need at least

$$\begin{aligned} m \geq \dim(\mathcal{A}+\mathcal{B}) &= \dim(\mathcal{A}) + \dim(\mathcal{B}) - \dim(\mathcal{A}\cap\mathcal{B}) \\ &= 2(d+t-1)r - r = (2(d+t)-3)r. \end{aligned}$$

Requirement on m

$$\mathcal{E} \subseteq \mathcal{V}_{d+t-1}.\mathcal{E} \cap \alpha^{-(d+t-1)}\mathcal{V}_{d+t-1}.\mathcal{E}$$
$$\mathcal{A} \quad \cap \quad \mathcal{B}$$

For equality we need at least

$$\begin{aligned} m \geq \dim(\mathcal{A}+\mathcal{B}) &= \dim(\mathcal{A}) + \dim(\mathcal{B}) - \dim(\mathcal{A}\cap\mathcal{B}) \\ &= 2(d+t-1)r - r = (2(d+t)-3)r. \end{aligned}$$

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_{t+1}(Z, A) + \Omega_{t+1}(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_{t+1}(Z, A) + \Omega_{t+1}(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_{t+1}(Z, A) + \Omega_{t+1}(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_{t+1}(Z, A) + \Omega_{t+1}(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A = \Omega_{t+1}(Z, A).$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t

Some properties of $\Omega_t(Z, A)$

$$\Omega_{t+1}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

If $\Omega_{t+1}(Z, A) = \Omega_t(Z, A)$ then $\Omega_{t'}(Z, A) = \Omega_t(Z, A)$ for all $t' \geq t$.

$$\Omega_{t+2}(Z, A) = \Omega_t(Z, A) + \Omega_t(Z, A)A$$

Since $\dim(\Omega_t(Z, A)) \leq r$, then $\Omega_t(Z, A) \subseteq \Omega_{r-1}(Z, A)$ for all t