MRD convolutional codes

Filipa Santana

Joint work with: Diego Napp and Raquel Pinto
My Team

Dra Raquel Pinto

Dr Diego Napp

CIDMA
Research Group
Coding Theory and the problem

In Information Theory the major concern is how to send a message from one source to one destination

Major problem: Error correction
Internet, Wireless network communications, Cloud computing

Network communications

brought new problems

Transmission of data from multiple sources to multiple receivers
Represent data in a matrix form and the rows of the matrix represent the packets sent through the channel.

The destination receives a linear combination of the different packets.
Very good approach when we have to send a lot of information or when we need to use the network several instants.

Correlation among the transmitted data in the different shots increases the correction capability of the code.
Rank metric codes

Rank metric codes are usually constructed as block codes of length $n$ over an extension field $\mathbb{F}_{q^m}$ and they have rate $\frac{km}{nm}$ (over $\mathbb{F}_q$).

$$u \in \mathbb{F}_{q^m}^k \quad \xrightarrow{} \quad v \in \mathbb{F}_{q^m}^n \quad \xrightarrow{} \quad V \in \mathbb{F}_q^{n \times m}$$

In our work we decided to use a more general approach:

The code $C$ is the image of the map $\varphi$ and has rate $\frac{k}{nm}$.

$$\varphi : \mathbb{F}_q^k \xrightarrow{\gamma} \mathbb{F}_q^{nm} \xrightarrow{\psi} \mathbb{F}_q^{n \times m}$$

$$u \xmapsto{\gamma} v = uG \xmapsto{\psi} V = \psi(v) \quad [3]$$

A different type of distance must be used in order to evaluate the error correction capability of the code.

The **rank distance of** $C$ is defined as

$$d_{\text{rank}}(C) = \min_{V \in C, V \neq 0} d_{\text{rank}}(V),$$

and if $C$ has rate $\frac{k}{nm}$ then

$$d_{\text{rank}}(C) \leq n - \left\lfloor \frac{k - 1}{m} \right\rfloor = n - \left\lfloor \frac{k}{m} \right\rfloor + 1. \quad \text{Singleton bound} \quad [4]$$

A code $C$ that attains the Singleton bound is called **Maximum Rank Distance (MRD).**

A rank metric convolutional code $\mathcal{C} \subset \mathbb{F}_q[D]^{n \times m}$ is defined as the image of the following map:

$$
\varphi : \mathbb{F}_q[D]^k \xrightarrow{\gamma} \mathbb{F}_q[D]^{nm} \xrightarrow{\psi} \mathbb{F}_q[D]^{n \times m}
$$

$$
u(D) \mapsto v(D) = u(D)G(D) \mapsto V(D), \quad [3]
$$

$\mathcal{C}$ is said to have rank $\frac{k}{mn}$ and $G(D) \in \mathbb{F}_q^{k \times nm}[D]$ is a full row rank polynomial matrix, called an encoder of $\mathcal{C}$.

The degree $\delta$ of a rank metric convolutional code $C$ is the minimum value of the sum of the row degrees of its encoders. Intimately related to the code distances and with the error correction capability of the code.

A rank metric convolutional code $C$ of rate $\frac{k}{nm}$ and degree $\delta$ is called an $(n \times m, k, \delta)$-rank metric convolutional code.
Sum rank distance of $\mathcal{C}$

If $\mathcal{C}$ is an $(n \times m, k, \delta)$ rank metric convolutional code, then the sum rank distance of $\mathcal{C}$ is given by

$$d_{SR}(\mathcal{C}) = \min_{0 \neq V(D) \in \mathcal{C}} \text{rwt}(V(D)).$$

And is upper bounded by

$$d_{SR}(\mathcal{C}) \leq n \left( \left\lceil \frac{\delta}{k} \right\rceil + 1 \right) - \left\lceil \frac{k \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \delta}{m} \right\rceil + 1.$$

An \((n \times m, k, \delta)\) rank metric convolutional code \(C\) such that:

\[
d_{SR}(C) = n \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \left\lfloor \frac{k(\left\lfloor \frac{\delta}{k} \right\rfloor + 1) - \delta}{m} \right\rfloor + 1.
\]

is called **Maximum Rank Distance (MRD)** convolutional code. [3]

**Contructions of MRD convolutional codes**

Napp, Pinto, Rosenthal and Vettori constructions and the ones proposed in this presentation
Constructions of MRD convolutional codes

In our work, we proposed new constructions of \((n \times m, k, \delta)\) MRD convolutional codes with larger values for the code degree \(\delta\) than the existing ones proposed by NPRV.

Let \(A \in \mathbb{F}_q^{m \times m}\) be a matrix with irreducible characteristic polynomial \(X(\lambda)\). Then the matrices \(A^i, i \in \{0, 1, \ldots, m - 1\}\) are \(\mathbb{F}_q\)-Linearly independent and

\[
\mathbb{F}_q[A] = \left\{ \sum_{i=0}^{m-1} u_i A^i : u_i \in \mathbb{F}_q, i = 0, \ldots, m - 1 \right\} \cong \mathbb{F}_{q^m}
\]

is a field.

Construction NPRV: An $(m \times m, 1, \delta)$ rank metric convolutional code $C$ with $\delta \leq m - 1$ and encoder

$$G(D) = \sum_{i=0}^{\delta} \psi^{-1}(A^i)D^i \in \mathbb{F}_q[D]^{1 \times m^2}$$

is MRD.

**Theorem:** The $(m \times m, 1, 2m - 1)$ rank metric convolutional code $C$, with encoder

$$G(D) = \sum_{i=0}^{m-1} \psi^{-1}(A^i)D^i + \sum_{i=0}^{\delta-m} \psi^{-1}(A^{m-1-i})D^{m+i} \in \mathbb{F}_q[D]^{1 \times m^2}, m \leq \delta \leq 2m - 1.$$ 

Is MRD.
Construction NPRV: An \((n \times m, k, \delta)\) rank metric convolutional code \(C\) with \(\delta \in \mathbb{N}_0\), such that \(k|\delta\), \(\delta \leq m - k\) and with encoder

\[
G(D) = \sum_{i=0}^{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} G_i D^i \in \mathbb{F}_q[D]^{k \times nm}
\]

Where,

\[
G_i = \begin{bmatrix}
\psi^{-1}(X A^{ki}) \\
\psi^{-1}(X A^{ki+1}) \\
\vdots \\
\psi^{-1}(X A^{ki+k-1})
\end{bmatrix}, \quad 0 \leq i \leq \frac{\delta}{k}, \quad \text{is MRD.}
\]
Theorem: The \((n \times m, k, 2\delta + k)\) rank metric convolutional code \(C\), with \(\delta \in \mathbb{N}_0\), such that \(k|\delta\), with encoder

\[
G(D) = \sum_{i=0}^{2\frac{\delta}{k}+1} G_i D^i \in \mathbb{F}_q[D]^{k \times nm},
\]

\[
G_i = \begin{bmatrix}
\psi^{-1}(XA^{ki}) \\
\psi^{-1}(XA^{ki+1}) \\
\vdots \\
\psi^{-1}(XA^{ki+k-1})
\end{bmatrix}, \quad 0 \leq i \leq \frac{\delta}{k}, \quad G_{\frac{\delta}{k}} = \begin{bmatrix}
0 & 1 \\
\vdots & \ddots \\
1 & 0
\end{bmatrix}, \quad G_{2\frac{\delta}{k}+1-i},
\]

for \(\frac{\delta}{k} + 1 \leq i \leq 2\frac{\delta}{k} + 1\).

is MRD.
Construction NPRV: An \((n \times m, k, \delta)\) rank metric convolutional code \(C\) with \(\delta \in \mathbb{N}_0\), such that \(k \nmid \delta, \delta \leq m - k\) and with encoder

\[
G(D) = \sum_{i=0}^{\left\lceil \frac{\delta}{k} \right\rceil + 1} G_i D^i \in \mathbb{F}_q[D]^{k \times nm}
\]

\[
G_i = \begin{bmatrix}
\psi^{-1}(XA^{ki}) \\
\psi^{-1}(XA^{ki+1}) \\
\vdots \\
\psi^{-1}(XA^{ki+k-1})
\end{bmatrix}, \quad 0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor 
\]

\[
G_{\left\lfloor \frac{\delta}{k} \right\rceil + 1} = \begin{bmatrix}
\psi^{-1}(XA^{k\left\lfloor \frac{\delta}{k} \right\rceil + k}) \\
\psi^{-1}(XA^{k+\delta-1}) \\
0 \\
\vdots \\
0
\end{bmatrix}
\]

is MRD.
**Theorem:** The \((n \times m, k, k \left(2 \left\lfloor \frac{\delta}{k} \right\rfloor + 3\right))\) rank metric convolutional code \(C\), with \(\delta \in \mathbb{N}_0\), such that \(k \nmid \delta\), with encoder

\[
G(D) = \sum_{i=0}^{2 \left\lfloor \frac{\delta}{k} \right\rfloor + 3} G_i D^i \in \mathbb{F}[D]^{k \times nm}
\]

\[
G_i = \begin{bmatrix}
\psi^{-1}(X A^{ki}) \\
\psi^{-1}(X A^{ki+1}) \\
\vdots \\
\psi^{-1}(X A^{ki+k-1})
\end{bmatrix}, \quad 0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor, \quad G_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} = \begin{bmatrix}
\psi^{-1}(X A^{k\left\lfloor \frac{\delta}{k} \right\rfloor + k}) \\
\vdots \\
\psi^{-1}(X A^{k+\delta-1}) \\
\psi^{-1}(XI) \\
\vdots \\
\psi^{-1}(X A^{k-1-(\delta-k\left\lfloor \frac{\delta}{k} \right\rfloor)})
\end{bmatrix}, \quad G_i = \begin{bmatrix}
0 & 1 \\
\vdots \\
1 & 0
\end{bmatrix} \quad G_{2 \left\lfloor \frac{\delta}{k} \right\rfloor + 3-i}, \quad \text{for } \left\lfloor \frac{\delta}{k} \right\rfloor + 2 \leq i \leq 2 \left\lfloor \frac{\delta}{k} \right\rfloor + 3.
\]

is MRD.
Hope to see you soon with more progress.