Criteria for the construction of MDS convolutional codes with good column distances

Julia Lieb

Institute of Mathematics
University of Zurich

Joint work with Zita Abreu, Raquel Pinto, Joachim Rosenthal

Convolutional Codes

Definition

A **convolutional code** $\mathcal{C}$ of **rate** k/n is a free $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$ of rank k.
There exists $G(z) \in \mathbb{F}[z]^{k \times n}$ of full row rank such that

$$\mathcal{C} = \{v \in \mathbb{F}[z]^n \mid v(z) = u(z)G(z) \text{ for some } u \in \mathbb{F}[z]^k\}.$$

$G(z)$ is called **generator matrix** of the code and is unique up to left multiplication with a unimodular matrix $U(z) \in Gl_k(\mathbb{F}[z])$.
The **degree** δ of $\mathcal{C}$ is defined as the maximal degree of the $k \times k$-minors of $G(z)$. One calls $\mathcal{C}$ an (n, k, δ) convolutional code.

Distances of Convolutional Codes

Definition

The **free distance** of a convolutional code $\mathcal{C}$ is defined as

$$d_{free}(\mathcal{C}) := min\{wt(v(z)) \mid v \in \mathcal{C} \text{ and } v \not\equiv 0\}.$$

For $j \in \mathbb{N}_0$, the **j-th column distance** of $\mathcal{C}$ is defined as

$$d_j^c(\mathcal{C}) := \min \left\{ \sum_{t=0}^{j} wt(v_t) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq 0 \right\}.$$

Distances of Convolutional Codes

Definition

The **free distance** of a convolutional code $\mathcal{C}$ is defined as

$$d_{free}(\mathcal{C}) := min\{wt(v(z)) \mid v \in \mathcal{C} \text{ and } v \not\equiv 0\}.$$

For $j \in \mathbb{N}_0$, the **j-th column distance** of $\mathcal{C}$ is defined as

$$d_j^c(\mathcal{C}) := \min \left\{ \sum_{t=0}^{j} wt(v_t) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq 0 \right\}.$$

Theorem (RS 1999, GRS 2006)

(i) $d_{free}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$

(ii) $d_j^c(\mathcal{C}) \leq (n-k)(j+1) + 1$

RS 1999: J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. Appl. Algebra Engrg. Comm. Comput., 10(1):15-32, 1999.
GRS 2006: H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. IEEE Trans. Inform. Theory, 52(2):584–598, 2006.

MDS and MDP Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n and degree δ is called
(i) **maximum distance separable (MDS)** if

$$d_{free}(\mathcal{C}) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1,$$

MDS and MDP Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n and degree δ is called
(i) **maximum distance separable (MDS)** if

$$d_{free}(\mathcal{C}) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1,$$

(ii) of **maximum distance profile (MDP)** if

$$d_j^c(\mathcal{C}) = (n-k)(j+1)+1 \quad \text{for } j = 0, \ldots, L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$$

MDS and MDP Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n and degree δ is called
(i) **maximum distance separable (MDS)** if

$$d_{free}(\mathcal{C}) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1,$$

(ii) of **maximum distance profile (MDP)** if

$$d_j^c(\mathcal{C}) = (n-k)(j+1)+1 \quad \text{for } j = 0, \ldots, L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$$

Lemma (GRS 2006)

Let $\mathcal{C}$ be an (n,k,δ) convolutional code with generator matrix $G(z)$ and G_0 full rank. If $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$ for some $j \in \{1, \ldots, L\}$, then $d_i^c(\mathcal{C}) = (n-k)(i+1)+1$ for all $i \leq j$.

Criteria for MDS convolutional codes - Preliminaries

Theorem (GRS 2006)

For an (n, k, δ) convolutional code $\mathcal{C}$ with $G(z) = \sum_{i=0}^{\mu} G_i z^i$ the following statements are equivalent:

(i) $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$

(ii) All fullsize minors of $G_j^c := \begin{bmatrix} G_0 & \dots & G_j \\ & \ddots & \vdots \\ 0 & & G_0 \end{bmatrix} \in \mathbb{F}^{k(j+1)\times n(j+1)}$

that are non trivially zero is nonzero.

Criteria for MDS convolutional codes - Preliminaries

Theorem (GRS 2006)

For an (n, k, δ) convolutional code $\mathcal{C}$ with $G(z) = \sum_{i=0}^{\mu} G_i z^i$ the following statements are equivalent:

(i) $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$

(ii) All fullsize minors of $G_j^c := \begin{bmatrix} G_0 & \dots & G_j \\ & \ddots & \vdots \\ 0 & & G_0 \end{bmatrix} \in \mathbb{F}^{k(j+1)\times n(j+1)}$

that are non trivially zero is nonzero.

Lemma

Let $A \in \mathbb{F}_q^{r\times s}$ with $r \leq s$ be such that all its fullsize minors are nonzero. Then, each vector which is a linear combination of the r rows of A has at least $s - r + 1$ nonzero entries.

Criteria for MDS convolutional codes - Idea

Let $u(z) \in \mathbb{F}_q^k[z]$ with $\deg(u) = \ell$ and $v(z) = u(z)G(z)$. Then, $(v_0 \ v_1 \ \cdots \ v_{\mu+\ell}) = (u_0 \ u_1 \ \cdots \ u_\ell)\mathcal{G}$, where

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_\mu & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & G_0 & \cdots & G_\mu \end{pmatrix} \qquad \text{for} \quad \ell > \mu$$

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_\ell & \cdots & G_\mu & & 0 \\ & \ddots & \vdots & & \vdots & \ddots & \\ 0 & & G_0 & \cdots & G_{\mu-\ell} & \cdots & G_\mu \end{pmatrix} \qquad \text{for} \quad \ell \leq \mu$$

We use that if $\mathcal{G} = [\mathcal{G}_1 \cdots \mathcal{G}_m]$, then

$$wt(v(z)) = \sum_{i=1}^{m} wt((u_0 \ u_1 \ \cdots \ u_\ell)\mathcal{G}_i).$$

Reverse Code

Definition

Let $\mathcal{C}$ be an (n, k, δ) convolutional code with generator matrix $G(z)$, which has entries $g_{ij}(z)$. Set $\overline{g}_{ij}(z) := z^{\nu_i} g_{ij}(z^{-1})$ where ν_i is the i-th row degree of $G(z)$. Then, the code $\overline{\mathcal{C}}$ with generator matrix $\overline{G}(z)$, which has $\overline{g}_{ij}(z)$ as entries, is called the **reverse code** to $\mathcal{C}$. We call the j-th column distance of $\overline{\mathcal{C}}$ the ***j*-th reverse column distance** of $\mathcal{C}$.

Remark

Let $G(z) = \sum_{i=0}^{\mu} G_i z^i$ and $\overline{G}(z) = \sum_{i=0}^{\mu} \overline{G}_i z^i$. If $k \mid \delta$, one has that $\overline{G}_i = G_{\mu-i}$ for $i = 0, \ldots, \mu$.

Criteria for MDS convolutional codes with $k \mid \delta$ - Idea

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_{\mu-1} & * & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & * & G_\mu & \ddots & \vdots \\ \vdots & \ddots & G_0 & * & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & * & G_1 & \cdots & G_\mu \end{pmatrix} \quad \text{for} \quad \ell \geq \mu - 1$$

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_{\ell-1} & G_\ell & \cdots & G_\mu & & 0 & \\ & \ddots & \vdots & \vdots & & \vdots & G_\mu & & \\ & & G_0 & \vdots & & \vdots & \vdots & \ddots & \\ 0 & & & G_0 & \cdots & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & G_\mu \end{pmatrix}$$

for $\ell < \mu - 1$.

ALPR 2023: Z. Abreu, J. Lieb, R. Pinto, J. Rosenthal. Criteria for the construction of MDS convolutional codes with good column distances, arXiv:2305.04647.

Criteria for MDS codes with $k \mid \delta$ - Results

Theorem (ALPR 2023)

Let $k \mid \delta$ and $G(z) = \sum_{i=0}^{\mu} G_i z^i$ with $\mu = \frac{\delta}{k}$. If $\mu \geq 3$, let $n \geq 3k - \frac{2k}{\delta - 2k}$, except for $k = 2, \delta = 6$ where we assume $n \geq 5$ and let all non trivially zero full-size minors of the following matrices be nonzero, where $0 \leq \ell < \min\left(\mu - 1, \frac{n(\mu+1)-k+1}{n+k}\right)$:

$$\begin{pmatrix} G_0 & \cdots & G_{\mu-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}, \begin{pmatrix} G_\mu & \cdots & G_1 \\ & \ddots & \vdots \\ 0 & & G_\mu \end{pmatrix} \text{ and } \begin{pmatrix} G_\ell & \cdots & G_\mu \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\mu-\ell} \end{pmatrix}.$$

If $\mu \leq 2$, let additionally all non trivially zero full-size minors of $\begin{pmatrix} G_0 & \cdots & G_\mu \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}$ be nonzero and assume for $\mu = 1$ that $n \geq 2k - 1$ and for $\mu = 2$ that $n \geq 3k - 2$.

Then, $\mathcal{C}$ is an MDS convolutional code.

Criteria for MDS convolutional codes with $k \nmid \delta$ - Idea

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_{\mu-1} & * & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & * & \tilde{G}_\mu & \ddots & \vdots \\ \vdots & \ddots & G_0 & * & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & * & G_1 & \cdots & \tilde{G}_\mu \end{pmatrix} \quad \text{for} \quad \ell \geq \mu - 1$$

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_{\ell-1} & G_\ell & \cdots & G_{\mu-1} & \tilde{G}_\mu & & 0 & \\ & \ddots & \vdots & \vdots & & \vdots & \vdots & \tilde{G}_\mu & & \\ & & G_0 & \vdots & & \vdots & \vdots & \vdots & \ddots & \\ 0 & & & G_0 & \cdots & G_{\mu-\ell-1} & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & \tilde{G}_\mu \end{pmatrix}$$

for $\ell < \mu - 1$.

Criteria for MDS codes with $k \nmid \delta$ - Results

Theorem (ALPR 2023)

Let $k \nmid \delta$ and let $\mathcal{C}$ be an (n, k, δ) convolutional code with minimal generator matrix $G(z)$ of degree $\mu = \lceil \frac{\delta}{k} \rceil$ and with generic row degrees. Denote by $\tilde{G}_\mu$ the matrix consisting of the (first) $t = \delta + k - k\mu$ nonzero rows of G_μ. If all not trivially zero full-size minors of the matrices

$$\begin{pmatrix} G_0 & \cdots & G_{\mu-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix} \text{ and } \begin{pmatrix} G_\ell & \cdots & G_{\mu-1} \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\mu-1-\ell} \end{pmatrix} \text{ for } 0 \leq \ell < \mu - 1$$

$$\text{and } \begin{pmatrix} \tilde{G}_\mu \\ G_{\mu-1} \\ \vdots \\ G_i \end{pmatrix} \text{ for } 0 < i \leq \mu - 1 \text{ s.t. } n \geq k(\mu - i + 1) \text{ and } \tilde{G}_\mu$$

are nonzero and $n \geq B$, then $\mathcal{C}$ is MDS.

Good column distances

Remark

If $k \mid \delta$, codes fulfilling our conditions are not only MDS but also reach the upper bound for the j-th column distance and the j-th reverse column distance until $j = \mu - 1$.

Remark

If $k \nmid \delta$, codes fulfilling our conditions reach the upper bound for the j-th column distance until $j = \mu - 1$. Moreover, $L = \mu - 1$ if and only if $n > \delta + k = k\mu + t$. In this case, $\mathcal{C}$ is also MDP.

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

Let S be the value of the generalized Singleton bound and set

$$W := \left\lceil \frac{S-2}{n-k} \right\rceil = \frac{\delta}{k} + 1 + \left\lceil \frac{\delta - 1}{n-k} \right\rceil, \; E := \left\lceil \frac{W}{2} \right\rceil - 1, \; F := \left\lfloor \frac{W}{2} \right\rfloor - 1.$$

If non-trivially zero full-size minors of G_E^c and $\bar{G}_F^c$ are nonzero, then $wt(u(z)G(z)) \geq S + R$ for all $u(z) \in \mathbb{F}[z]^k$ with $\deg(u) \geq E$.

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

Let S be the value of the generalized Singleton bound and set

$$W := \left\lceil \frac{S-2}{n-k} \right\rceil = \frac{\delta}{k} + 1 + \left\lceil \frac{\delta - 1}{n-k} \right\rceil, \ E := \left\lceil \frac{W}{2} \right\rceil - 1, \ F := \left\lfloor \frac{W}{2} \right\rfloor - 1.$$

If non-trivially zero full-size minors of G_E^c and $\bar{G}_F^c$ are nonzero, then $wt(u(z)G(z)) \geq S + R$ for all $u(z) \in \mathbb{F}[z]^k$ with $\deg(u) \geq E$.

If $R \geq F \cdot k - 1$, we consider $\left(\begin{array}{ccc|c} G_\mu & \cdots & G_{\mu-F+1} & G_{\mu-F} \\ & \ddots & \vdots & \vdots \\ & & G_\mu & G_{\mu-1} \\ & & & G_\mu \end{array}\right)$

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

Let S be the value of the generalized Singleton bound and set

$$W := \left\lceil \frac{S-2}{n-k} \right\rceil = \frac{\delta}{k} + 1 + \left\lceil \frac{\delta - 1}{n-k} \right\rceil, \; E := \left\lceil \frac{W}{2} \right\rceil - 1, \; F := \left\lfloor \frac{W}{2} \right\rfloor - 1.$$

If non-trivially zero full-size minors of G_E^c and $\bar{G}_F^c$ are nonzero, then $wt(u(z)G(z)) \geq S + R$ for all $u(z) \in \mathbb{F}[z]^k$ with $\deg(u) \geq E$.

If $R \geq F \cdot k - 1$, we consider $\left(\begin{array}{cccc|c} G_\mu & \cdots & G_{\mu-F+1} & & G_{\mu-F} \\ & \ddots & \vdots & & \vdots \\ & & G_\mu & & G_{\mu-1} \\ & & & & G_\mu \end{array}\right)$

and if $R - F \cdot k + 1 \geq E \cdot k - 1$, $\left(\begin{array}{cccc|c} G_0 & \cdots & G_{E-1} & & G_E \\ & \ddots & \vdots & & \vdots \\ & & G_0 & & G_1 \\ & & & & G_0 \end{array}\right)$

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

If $\ell = \deg(u) < F \leq \mu - 1$, we write $wt(v(z)) = S + A$.
If $A \geq k$, we consider

$$\left(\begin{array}{ccc|c|ccc|ccc}
G_0 & \cdots & G_{\ell-1} & G_\ell & G_{\ell+1} & \cdots & G_\mu & & & \\
 & \ddots & \vdots & \vdots & \vdots & & \vdots & G_\mu & & \\
 & & G_0 & \vdots & \vdots & & \vdots & \vdots & \ddots & \\
 & & & G_0 & G_1 & \cdots & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & G_\mu
\end{array}\right)$$

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

If $\ell = \deg(u) < F \leq \mu - 1$, we write $wt(v(z)) = S + A$.
If $A \geq k$, we consider

$$\left(\begin{array}{ccc|c|ccc|ccc}
G_0 & \cdots & G_{\ell-1} & G_\ell & G_{\ell+1} & \cdots & G_\mu & & & \\
 & \ddots & \vdots & \vdots & \vdots & & \vdots & G_\mu & & \\
 & & G_0 & \vdots & \vdots & & \vdots & \vdots & \ddots & \\
 & & & G_0 & G_1 & \cdots & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & G_\mu
\end{array}\right)$$

If even $A \geq 2k$, we can consider the splitting

$$\left(\begin{array}{ccc|ccc|ccc}
G_0 & \cdots & G_\ell & G_{\ell+1} & \cdots & G_{\mu-1} & G_\mu & & \\
 & \ddots & \vdots & \vdots & & \vdots & \vdots & \ddots & \\
 & & G_0 & G_1 & \cdots & G_{\mu-\ell-1} & G_{\mu-\ell} & \cdots & G_\mu
\end{array}\right)$$

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

If $\ell = \deg(u) < F \leq \mu - 1$, we write $wt(v(z)) = S + A$.
If $A \geq k$, we consider

$$\left(\begin{array}{ccc|c|ccc|ccc}
G_0 & \cdots & G_{\ell-1} & G_\ell & G_{\ell+1} & \cdots & G_\mu & & & \\
 & \ddots & \vdots & \vdots & \vdots & & \vdots & G_\mu & & \\
 & & G_0 & \vdots & \vdots & & \vdots & \vdots & \ddots & \\
 & & & G_0 & G_1 & \cdots & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & G_\mu
\end{array}\right)$$

If even $A \geq 2k$, we can consider the splitting

$$\left(\begin{array}{ccc|ccc|ccc}
G_0 & \cdots & G_\ell & G_{\ell+1} & \cdots & G_{\mu-1} & G_\mu & & \\
 & \ddots & \vdots & \vdots & & \vdots & \vdots & \ddots & \\
 & & G_0 & G_1 & \cdots & G_{\mu-\ell-1} & G_{\mu-\ell} & \cdots & G_\mu
\end{array}\right)$$

We can split the middle matrix $x = \min\left(\mu - \ell - 2, \left\lfloor \frac{A-2k}{(\ell+1)k-1} \right\rfloor\right)$ times.
If $x = \mu - \ell - 2$, delete $y = \min\left(\mu - \ell - 1, \left\lfloor \frac{A-2k-(\mu-\ell-2)((\ell+1)k-1)}{n-(\ell+1)k+1} \right\rfloor\right)$ matrices.

Optimizing conditions for given n, k, δ (for $k \mid \delta$)

If $\ell = \deg(u) < F \leq \mu - 1$, we write $wt(v(z)) = S + A$.
If $A \geq k$, we consider

$$\left(\begin{array}{ccc|c|ccc|ccc} G_0 & \cdots & G_{\ell-1} & G_\ell & G_{\ell+1} & \cdots & G_\mu & & & \\ & \ddots & \vdots & \vdots & \vdots & & \vdots & G_\mu & & \\ & & G_0 & \vdots & \vdots & & \vdots & \vdots & \ddots & \\ & & & G_0 & G_1 & \cdots & G_{\mu-\ell} & G_{\mu-\ell+1} & \cdots & G_\mu \end{array}\right)$$

If even $A \geq 2k$, we can consider the splitting

$$\left(\begin{array}{ccc|ccc|ccc} G_0 & \cdots & G_\ell & G_{\ell+1} & \cdots & G_{\mu-1} & G_\mu & & \\ & \ddots & \vdots & \vdots & & \vdots & \vdots & \ddots & \\ & & G_0 & G_1 & \cdots & G_{\mu-\ell-1} & G_{\mu-\ell} & \cdots & G_\mu \end{array}\right)$$

We can split the middle matrix $x = \min\left(\mu - \ell - 2, \left\lfloor \frac{A-2k}{(\ell+1)k-1} \right\rfloor\right)$ times.
If $x = \mu - \ell - 2$, delete $y = \min\left(\mu - \ell - 1, \left\lfloor \frac{A-2k-(\mu-\ell-2)((\ell+1)k-1)}{n-(\ell+1)k+1} \right\rfloor\right)$ matrices.
The case $\ell = F = E - 1$ has to be considered separately.

Example

Let $k = 2$, $n = 11$, $\delta = 6$, i.e. $\mu = 3$, $S = 43$ and $E = 2$, $F = 1$. Then, $R = 4 \geq Fk - 1 + Ek - 1$, i.e. from $\ell \geq E$ we obtain

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, G_3.$$

Example

Let $k = 2$, $n = 11$, $\delta = 6$, i.e. $\mu = 3$, $S = 43$ and $E = 2$, $F = 1$. Then, $R = 4 \geq Fk - 1 + Ek - 1$, i.e. from $\ell \geq E$ we obtain

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, G_3.$$

For $\ell = 1 = F = E - 1$, we start with G_0, $\begin{pmatrix} G_1 & G_2 & G_3 \\ G_0 & G_1 & G_2 \end{pmatrix}$, G_3. As $A = 7 \geq 2k$, we change to $\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, \begin{pmatrix} G_3 & 0 \\ G_2 & G_3 \end{pmatrix}$ and since $A - 2k = 4 \geq Fk - 1$, we can obtain the splitting

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, G_3.$$

Example

Let $k = 2$, $n = 11$, $\delta = 6$, i.e. $\mu = 3$, $S = 43$ and $E = 2$, $F = 1$. Then, $R = 4 \geq Fk - 1 + Ek - 1$, i.e. from $\ell \geq E$ we obtain

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, G_3.$$

For $\ell = 1 = F = E - 1$, we start with G_0, $\begin{pmatrix} G_1 & G_2 & G_3 \\ G_0 & G_1 & G_2 \end{pmatrix}$, G_3. As $A = 7 \geq 2k$, we change to $\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, \begin{pmatrix} G_3 & 0 \\ G_2 & G_3 \end{pmatrix}$ and since $A - 2k = 4 \geq Fk - 1$, we can obtain the splitting

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, G_3.$$

Clearly, $x = 0$ and as also $y = 0$ in sum the non trivially zero full-size minors of the following matrices have to be nonzero:

$$\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_3 \end{pmatrix}, \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, [G_0\ G_1\ G_2\ G_3].$$

Construction of MDS convolutional codes

Definition

Let $r, n, m \in \mathbb{N}$ and consider a Toeplitz matrix

$A \in \mathbb{F}_q^{(r+1)n\times(r+1)m}$ of the form $A = \begin{pmatrix} A_0 & \cdots & A_r \\ & \ddots & \vdots \\ 0 & & A_0 \end{pmatrix}$ with

$A_i \in \mathbb{F}_q^{n\times m}$ for $i \in \{0, \dots, r\}$. A is called **reverse superregular Toeplitz matrix** if all non trivially zero minors (of any size) of

the matices A and $A_{rev} = \begin{pmatrix} A_r & \cdots & A_0 \\ & \ddots & \vdots \\ 0 & & A_r \end{pmatrix}$ are nonzero.

Remark

Our conditions for $k \mid \delta$ *are fulfilled if* G_μ^c *is a reverse superregular Toeplitz matrix and with slight adaption this can be also used for the case that* $k \nmid \delta$*. However, using this for the construction of MDS codes leads to very large field sizes.*

Construction of MDS convolutional codes

Theorem (ALPR 2023)

Let $n, k, \delta \in \mathbb{N}$ such that they fulfill our conditions and let α be a primitive element of a finite field $\mathbb{F} = \mathbb{F}_{p^N}$ with $N > \mu \cdot 2^{(\mu+1)n+t-1}$. Then $G(z) = \sum_{i=0}^{\mu} G_i z^i$ with

$$G_i = \begin{bmatrix} \alpha^{2^{in}} & \dots & \alpha^{2^{(i+1)n-1}} \\ \vdots & & \vdots \\ \alpha^{2^{in+k-1}} & \dots & \alpha^{2^{(i+1)n+k-2}} \end{bmatrix}$$

for $i = 0, \dots, \mu - 1$ and

$$\tilde{G}_\mu = \begin{pmatrix} \alpha^{2^{\mu n}} & \dots & \alpha^{2^{(\mu+1)n-1}} \\ \vdots & & \vdots \\ \alpha^{2^{\mu n+t-1}} & \dots & \alpha^{2^{(\mu+1)n+t-2}} \end{pmatrix}$$

is the generator matrix of an MDS convolutional code.

Construction Examples

Example

If $k = \delta = 1$, i.e. $\mu = 1$ and n arbitrary, one obtains $E = F = 0$. Hence, it is enough if all full-size minors, i.e. all entries, of G_0 and G_1 are nonzero. This means $G_0 = G_1 = (1 \ \cdots \ 1)$ defines an MDS convolutional code over any field.

Construction Examples

Example

If $k = \delta = 1$, i.e. $\mu = 1$ and n arbitrary, one obtains $E = F = 0$. Hence, it is enough if all full-size minors, i.e. all entries, of G_0 and G_1 are nonzero. This means $G_0 = G_1 = (1 \ \cdots \ 1)$ defines an MDS convolutional code over any field.

Example

If $k = 1$, $\delta = 2$ and n arbitrary, $E = F = 1$, i.e. all non trivially zero full-size minors of $(G_0 \ G_1 \ G_2)$, $\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}$ and $\begin{pmatrix} G_2 & G_1 \\ 0 & G_2 \end{pmatrix}$ have to be nonzero. Hence, an $(n, 1, 2)$ MDS convolutional code exists for $q \geq n + 1$, e.g. $G_0 = G_2 = (1 \ \cdots \ 1)$ and $G_1 = (1 \ \alpha \ \cdots \alpha^{n-1})$ where α is a primitive element of $\mathbb{F}_q$. For $n = 2$ this field size is smaller than in previous constructions, for $n \geq 3$ it is equal to the best previous construction.

Construction Examples

Example

For $k = 1$, $n = \delta = 3$, i.e. $\mu = 3$ and $S = 12$, the best existing constructions require $q \geq 10$. Our criterion requires that the non trivially zero full-size minors of the following matrices are nonzero:

$$G_2^c,\ \overline{G}_1^c,\ \begin{pmatrix} G_2 \\ G_1 \end{pmatrix},\ [G_0\ G_1\ G_2\ G_3].$$

Using this, we found an $(3, 1, 3)$ MDS convolutional code over $\mathbb{F}_7$ defined by the generator matrix $G(z) = \sum_{i=0}^{3} G_i z^i$, with $G_0 = (4\ 4\ 2)$, $G_1 = (1\ 4\ 3)$, $G_2 = (4\ 6\ 2)$ and $G_3 = (1\ 2\ 1)$, which additionally has optimal j-th column distance for $j \leq 2$ and optimal reverse column distance for $j \leq 1$.

Construction Examples

Example

For $k = 2,\ \delta = 4,\ n = 5$, i.e. $\mu = 2$ and $S = 14$, we get the conditions that all non trivially zero full-size minors of the matrices $\begin{pmatrix} G_0 & G_1 & G_2 \end{pmatrix}$, G_1^c and $\overline{G}_1^c$ have to be nonzero. We found the following solution over $\mathbb{F}_{31}$:

$G_0 = \begin{pmatrix} 5 & 30 & 14 & 11 & 1 \\ 3 & 23 & 21 & 12 & 5 \end{pmatrix}$, $G_1 = \begin{pmatrix} 17 & 4 & 24 & 14 & 7 \\ 7 & 24 & 12 & 20 & 22 \end{pmatrix}$

and $G_2 = \begin{pmatrix} 14 & 0 & 12 & 19 & 1 \\ 23 & 1 & 21 & 1 & 22 \end{pmatrix}$.

In previous constructions smallest possible field size is 31 as well. However, our code has the additional advantage that for $j \in \{0, 1\}$, the j-th column distance and the j-th reverse column distance are optimal.

Example

Let $k = 2$, $n = 3$ and $\delta = 3$, i.e. $\mu = 2$ and $t = 1$. We get the conditions that all non trivially zero full-size minors of G_1^c, G_1 and $\tilde{G}_2$ have to be nonzero. The following example over $\mathbb{F}_3$ fulfills these conditions:

$$G_0 = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 2 \end{pmatrix}, \; G_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix}, \; G_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

The smallest possible field in previous constructions with these parameters is $\mathbb{F}_{16}$. This means we manage to improve the field size a lot and additionally, our code has optimal j-th column distance for $j \in \{0, 1\}$.

Example

Let $k = 2$, $n = 6$ and $\delta = 3$, i.e. $\mu = 2$ and $t = 1$. We need that all full-size minors of G_0, $\begin{pmatrix} G_1 \\ G_0 \end{pmatrix}$, G_1 and $\tilde{G}_2$ are nonzero. An example fulfilling these conditions over $\mathbb{F}_7$ is

$$G_0 = \begin{pmatrix} 2 & 5 & 6 & 2 & 2 & 0 \\ 6 & 5 & 5 & 0 & 3 & 4 \end{pmatrix}, G_1 = \begin{pmatrix} 4 & 6 & 4 & 4 & 5 & 5 \\ 1 & 4 & 0 & 2 & 5 & 2 \end{pmatrix},$$
$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The smallest possible field in previous constructions with these parameters is $\mathbb{F}_{16}$.

Conclusion

- We presented new (sufficient) criteria for the construction of MDS convolutional codes, considering certain minors of the sliding generator matrix of the code

Conclusion

- We presented new (sufficient) criteria for the construction of MDS convolutional codes, considering certain minors of the sliding generator matrix of the code
- We presented a general construction for MDS convolutional codes with good column distances (over large finite fields)

Conclusion

- We presented new (sufficient) criteria for the construction of MDS convolutional codes, considering certain minors of the sliding generator matrix of the code
- We presented a general construction for MDS convolutional codes with good column distances (over large finite fields)
- We presented some construction examples for MDS convolutional codes over fields of smaller size than in previous constructions with the same code parameters