A novel criterion for the construction of MDS convolutional codes of rate $1/n$

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

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

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 $i \leq j$.

Known Constructions for MDS convolutional codes of rate $1/n$

- J. Justesen. An algebraic construction of rate $1/\nu$ convolutional codes. IEEE Trans. Inform. Theory, IT-21(1):577–580, 1975.
- H. Gluesing-Luerssen and B. Langfeld. A class of one-dimensional mds convolutional codes. Journal of Algebra and Its Applications, 5(4):505–520, 2006.
- R. Smarandache and J. Rosenthal. A state space approach for constructing MDS rate 1/n convolutional codes. In Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory, pages 116–117, Killarney, Kerry, Ireland, June 1998.

MDP convolutional codes

Definition

For $r \in \mathbb{N}$, let $A = [a_{ij}] \in \mathbb{F}_q^{r \times r}$. Define $X = \{x_{ij} : i, j \in \{1, \ldots, r\}\}$ and let $\mathbb{F}_q[X]$ be the set of polynomials in the indeterminates x_{ij}.

Then, define $\overline{A} \in \mathbb{F}_q[X]^{r \times r}$ via $\quad \overline{a}_{ij} = \begin{cases} 0 & \text{for } a_{ij} = 0 \\ x_{ij} & \text{for } a_{ij} \neq 0 \end{cases}$.

The determinant of A is called **trivially zero** if $\det(\overline{A})$ is equal to the zero polynomial and it is called **non trivially zero** otherwise.

MDP convolutional codes

Definition

For $r \in \mathbb{N}$, let $A = [a_{ij}] \in \mathbb{F}_q^{r\times r}$. Define $X = \{x_{ij} : i, j \in \{1, \ldots, r\}\}$ and let $\mathbb{F}_q[X]$ be the set of polynomials in the indeterminates x_{ij}.

Then, define $\overline{A} \in \mathbb{F}_q[X]^{r\times r}$ via $\quad \overline{a}_{ij} = \begin{cases} 0 & \text{for } a_{ij} = 0 \\ x_{ij} & \text{for } a_{ij} \neq 0 \end{cases}$.

The determinant of A is called **trivially zero** if $\det(\overline{A})$ is equal to the zero polynomial and it is called **non trivially zero** otherwise.

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

that are non trivially zero is nonzero.

Criteria for MDS convolutional codes - Preliminaries

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 $\mathcal{C}$.

Remark

For $k = 1$, the reverse code $\overline{\mathcal{C}}$ to $\mathcal{C}$ with generator matrix $G(z) = \sum_{i=0}^{\delta} G_i z^i$ has generator matrix $\overline{G}(z) = \sum_{i=0}^{\delta} G_{\delta - i} z^i$.

Criteria for MDS convolutional codes - Preliminaries

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 $\mathcal{C}$.

Remark

For $k = 1$, the reverse code $\overline{\mathcal{C}}$ to $\mathcal{C}$ with generator matrix $G(z) = \sum_{i=0}^{\delta} G_i z^i$ has generator matrix $\overline{G}(z) = \sum_{i=0}^{\delta} G_{\delta - i} z^i$.

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 - Theorem

Theorem (ALPR 2023)

Consider an $(n, 1, \delta)$ *convolutional code* $\mathcal{C}$ *with* $n = 2$ *and* $\delta \leq 4$ *or* $n \geq 3$ *and* δ *arbitrary and generator matrix* $G(z) = \sum_{i=0}^{\delta} G_i z^i$. *Assume that all non trivially zero fullsize minors of the following matrices are nonzero:*

$$\begin{pmatrix} G_0 & \cdots & G_{\delta-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix} \text{ and } \begin{pmatrix} G_\delta & \cdots & G_1 \\ & \ddots & \vdots \\ 0 & & G_\delta \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} G_\ell & \cdots & G_\delta \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\delta-\ell} \end{pmatrix} \text{ for } 0 \leq \ell < \min\left(\delta - 1, \frac{n(\delta+2)}{n+1}\right).$$

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

Criteria for MDS convolutional codes - Proof

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

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

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

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

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

Criteria for MDS convolutional codes - Proof

If $\mathcal{G} = [\mathcal{G}_1 \cdots \mathcal{G}_m]$, then $wt(v(z)) = \sum_{i=1}^{m} wt((u_0\ u_1\ \cdots\ u_\ell)\mathcal{G}_i)$. where

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

As we can assume $u_0 \neq 0 \neq u_\ell$, we can conclude

$$wt(v(z)) \geq 2\big((n-1)\delta+1\big) = n(\delta+1)+n(\delta-1)-2(\delta-1) \geq n(\delta+1).$$

Criteria for MDS convolutional codes - Proof

If $\mathcal{G} = [\mathcal{G}_1\ \mathcal{G}_2\ \mathcal{G}_3]$, then $wt(v(z)) = \sum_{i=1}^{3} wt((u_0\ u_1\ \cdots\ u_\ell)\mathcal{G}_i)$. where

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

for $\ell < \delta - 1$.

$$\begin{aligned} wt(v(z)) &\geq 2\big((n-1)\ell + 1\big) + n(\delta - \ell + 1) - (\ell + 1) + 1 \\ &= n(\delta + 1) + n\ell - 3\ell + 2 \geq n(\delta + 1) \end{aligned}$$

for $n \geq 3$ or $n = 2$ and $\ell \leq \delta - 2 \leq 2$.

Construction of MDS 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 $i \in \{0, \ldots, r\}$. 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

All conditions of the preceding Theorem are fulfilled if G_δ^c is a reverse superregular Toeplitz matrix. However, using this for the construction of MDS codes leads to very large field sizes.

Examples

Example

For $\delta = 2$, our criterion says that all non trivially zero fullsize 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.

We obtain $(n, 1, 2)$ MDS convolutional code for $q \geq n + 1$, e.g. $G_0 = G_2 = (1\ \cdots\ 1)$ and $G_1 = (1\ \alpha\ \cdots \alpha^{n-1})$ with α primitive element of $\mathbb{F}_q$.

For $n = 2$ this field size is smaller than in existing constructions, for $n \geq 3$ it is equal to the best existing construction.

Examples

Example

For $n = \delta = 3$, the best existing constructions require $q \geq 10$. We found via computer search that the smallest possible field such that the conditions of the preceding theorem are fullfiled is $\mathbb{F}_{16}$. To improve the field size, we look where in the proof of the theorem our estimations were not sharp and realize that in case $\ell = 1$, we get weight 3 from G_1^c and $\bar{G}_1^c$, respectively. Hence, we only need weight 6 coming from the part $\begin{pmatrix} G_1 & G_2 & G_3 \\ G_0 & G_1 & G_2 \end{pmatrix}$. For this it is enough if all fullsize minors of the three separated matrices $\begin{pmatrix} G_1 \\ G_0 \end{pmatrix}$ and $\begin{pmatrix} G_2 \\ G_1 \end{pmatrix}$ and $\begin{pmatrix} G_3 \\ G_2 \end{pmatrix}$ and are nonzero. With this modified version of the theorem, 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 $G_0 = (4\ 4\ 5)$, $G_1 = (6\ 5\ 3)$, $G_2 = (3\ 2\ 6)$ and $G_3 = (5\ 3\ 4)$.

Outlook/Future work

- Investigate to which extent we can release the conditions of our main theorem depending on the code parameters to obtain construction examples for MDS convolutional codes over smaller fields

Outlook/Future work

- Investigate to which extent we can release the conditions of our main theorem depending on the code parameters to obtain construction examples for MDS convolutional codes over smaller fields
- Generalization of the results to convolutional codes with $k > 1$.

Thank you!