Convolutional codes over finite rings

Raquel Pinto

CIDMA, University of Aveiro, Portugal

5 ICM CTA

28-31 August 2017

International Castle Meeting on Coding Theory and Applications

Overview

- Convolutional codes over finite fields
- Convolutional codes over $\mathbb{Z}_{p^r}$, where p is a prime integer and $r > 1$
- Dual code

Block codes vs convolutional codes

$$\ldots u_2,\ u_1,\ u_0 \xrightarrow{\quad G \quad} \ldots v_2 = u_2 G,\ v_1 = u_1 G,\ v_0 = u_0 G$$

represented in a polynomial way

$$\cdots + u_2 D^2 + u_1 D + u_0 \xrightarrow{\quad G \quad} \cdots + \underbrace{u_2 G}_{v_2} D^2 + \underbrace{u_1 G}_{v_1} D + \underbrace{u_0 G}_{v_0}$$

Block codes vs convolutional codes

$$\dots u_2,\ u_1,\ u_0 \xrightarrow{\quad G \quad} \dots v_2 = u_2 G,\ v_1 = u_1 G,\ v_0 = u_0 G$$

represented in a polynomial way

$$\dots + u_2 D^2 + u_1 D + u_0 \xrightarrow{\quad G \quad} \dots + \underbrace{u_2 G}_{v_2} D^2 + \underbrace{u_1 G}_{v_1} D + \underbrace{u_0 G}_{v_0}$$

Substitute G by $G(D) = G_0 + G_1 D + \dots + G_s D^s$ [Elias, 1955]:

$$\dots u_2 D^2 + u_1 D + u_0 \xrightarrow{\color{red}{G(D)}} \dots \underbrace{(u_2 G_0 + u_1 G_1 + u_0 G_2)}_{v_2} D^2 + \underbrace{(u_1 G_0 + u_0 G_1)}_{v_1} D + \underbrace{u_0 G_0}_{v_0}$$

Block codes vs convolutional codes

$$\dots u_2,\ u_1,\ u_0 \xrightarrow{\quad G \quad} \dots v_2 = u_2 G,\ v_1 = u_1 G,\ v_0 = u_0 G$$

represented in a polynomial way

$$\cdots + u_2 D^2 + u_1 D + u_0 \xrightarrow{\quad G \quad} \cdots + \underbrace{u_2 G}_{v_2} D^2 + \underbrace{u_1 G}_{v_1} D + \underbrace{u_0 G}_{v_0}$$

Substitute G by $G(D) = G_0 + G_1 D + \cdots + G_s D^s$ [Elias, 1955]:

$$\dots u_2 D^2 + u_1 D + u_0 \xrightarrow{G(D)} \dots \underbrace{(u_2 G_0 + u_1 G_1 + u_0 G_2)}_{v_2} D^2 + \underbrace{(u_1 G_0 + u_0 G_1)}_{v_1} D + \underbrace{u_0 G_0}_{v_0}$$

Block codes: $\mathcal{C} = \{uG\} = \mathrm{Im}_{\mathbb{F}} G \sim \{u(D)G\} = \mathrm{Im}_{\mathbb{F}[D]} G$
Convolutional codes: $\mathcal{C} = \{u(D)G(D)\} = \mathrm{Im}_{\mathbb{F}[D]} G(D)$

Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ is an $\mathbb{F}[D]$-submodule of $\mathbb{F}^n[D]$.

Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ is an $\mathbb{F}[D]$-submodule of $\mathbb{F}^n[D]$.

A matrix $G(D)$ whose rows form a basis for $\mathcal{C}$ is called an encoder.
If $\mathcal{C}$ has rank k then we say that $\mathcal{C}$ has rate k/n.

$$\mathcal{C} \quad = \quad \mathrm{Im}_{\mathbb{F}[D]} G(D) = \left\{ u(D)G(D) : \; u(D) \in \mathbb{F}^k[D] \right\}\}$$

Any other encoder of $\mathcal{C}$ can be obtained by $\tilde{G}(D) = U(D)G(D)$, where $U(D) \in \mathbb{F}^{k \times k}[D]$ is unimodular (i.e., it admits an inverse in $\mathbb{F}^{k \times k}[D]$).

Any other encoder of $\mathcal{C}$ can be obtained by $\tilde{G}(D) = U(D)G(D)$, where $U(D) \in \mathbb{F}^{k\times k}[D]$ is unimodular (i.e., it admits an inverse in $\mathbb{F}^{k\times k}[D]$).

An encoder $G(D) \in \mathbb{F}^{k\times n}[D]$ is left prime if

$$G(D) = L(D)\tilde{G}(D),\ L(D) \in \mathbb{F}^{k\times k}[D], \tilde{G}(D) \in \mathbb{F}^{k\times n}[D] \Rightarrow$$

$\Rightarrow L(D)$ unimodular.

If $\mathcal{C}$ admits a left prime encoder then all its encoders are left prime $\rightarrow \mathcal{C}$ is called observable.

A full column rank matrix $H(D) \in \mathbb{F}^{n\times(n-k)}[D]$ is a parity-check matrix of $\mathcal{C}$ if

$$v(D) \in \mathcal{C} \;\Leftrightarrow\; v(D)H(D) = 0.$$

i.e. $\mathcal{C} = \ker_{\mathbb{F}[D]} H(D)$ and $\mathcal{C}^{\perp} = \mathrm{Im}_{\mathbb{F}[D]} H(D)^T$ is the dual code of $\mathcal{C}$.

Theorem

A convolutional code $\mathcal{C}$ admits a parity-check matrix if and only if it is observable.

After channel transmission: to check if the received word $v(D)$ belongs to $\mathcal{C}$:

$$v(D)H(D) = 0 \Rightarrow v(D) \in \mathcal{C}.$$

After channel transmission: to check if the received word $v(D)$ belongs to $\mathcal{C}$:

$$v(D)H(D) = 0 \Rightarrow v(D) \in \mathcal{C}.$$

Erasure channel: a symbol arrives correctly or does not arrive (erasure)

$$v(D) \in \mathcal{C} \Rightarrow v(D)H(D) = 0$$

It is enough to find $H(D)$ such that $\mathcal{C} \subset \ker_{\mathbb{F}[D]} H(D)$!

$$
\begin{array}{rcl}
\mathcal{C} = \mathrm{Im}_{\mathbb{F}[D]} G(D) \quad \subset \quad \tilde{\mathcal{C}} & = & \mathrm{Im}_{\mathbb{F}((D))} G(D) \\
 & = & \{u(D)G(D) : u(D) \in \mathbb{F}^k((D))\}
\end{array}
$$

where $\mathbb{F}((D)) = \{\sum_{i=k}^{+\infty} a_i D^i : a_i \in \mathbb{F}, k \in \mathbb{Z}\}$ is a field ($\mathbb{F}[D] \subset \mathbb{F}((D))$).

$$\begin{array}{rcl}\mathcal{C} = \mathrm{Im}_{\mathbb{F}[D]} G(D) \quad \subset \quad \tilde{\mathcal{C}} & = & \mathrm{Im}_{\mathbb{F}((D))} G(D) \\ & = & \{u(D)G(D) : u(D) \in \mathbb{F}^k((D))\}\end{array}$$

where $\mathbb{F}((D)) = \{\sum_{i=k}^{+\infty} a_i D^i : a_i \in \mathbb{F}, k \in \mathbb{Z}\}$ is a field ($\mathbb{F}[D] \subset \mathbb{F}((D))$).

$$\mathcal{C} \subset \tilde{\mathcal{C}} = \ker_{\mathbb{F}((D))} \; H(D)$$

for some full column rank $H(D) \in \mathbb{F}[D]^{n \times (n-k)}$

$$v(D) \in \mathcal{C} \Rightarrow v(D)H(D) = 0$$

Example

$$\begin{aligned}\mathcal{C} = \mathrm{Im}_{\mathbb{F}_2[D]}[1+D \;\; 1+D] \quad \subset \quad \tilde{\mathcal{C}} \quad &= \quad \mathrm{Im}_{\mathbb{F}_2((D))}[1+D \;\; 1+D] \\ &= \quad \ker_{\mathbb{F}_2((D))} \begin{bmatrix} 1 \\ -1 \end{bmatrix}\end{aligned}$$

Note: $[1 \;\; 1] \notin \mathcal{C}$ but $[1 \;\; 1] \in \tilde{\mathcal{C}}$!

Example

$$\begin{aligned} \mathcal{C} = \mathrm{Im}_{\mathbb{F}_2[D]}[1+D \;\; 1+D] \quad \subset \quad \tilde{\mathcal{C}} \quad &= \quad \mathrm{Im}_{\mathbb{F}_2((D))}[1+D \;\; 1+D] \\ &= \quad \ker_{\mathbb{F}_2((D))} \left[\begin{array}{c} 1 \\ -1 \end{array} \right] \end{aligned}$$

Note: $[1 \;\; 1] \notin \mathcal{C}$ but $[1 \;\; 1] \in \tilde{\mathcal{C}}$!

Received word: $v(D) = [1 + D^2 \;\; *]$

$$v(D)H(D) = 0 \;\Leftrightarrow\; [1 + D^2 \;\; *] \left[\begin{array}{c} 1 \\ -1 \end{array} \right] = 0 \;\Leftrightarrow\; * = 1 + D^2$$

Row reduced encoders

Let $v(D)$ be a nonzero vector in $\mathbb{F}^n[D]$:

$$v(D) = v_0 + v_1 D + \cdots + v_\nu D^\nu,$$

with $v_i \in \mathbb{F}^n$, $i = 0, \ldots, \nu$, and $v_\nu \neq 0$.

- $v(D)$ has **degree** ν, $deg\, v(D) = \nu$;
- v_ν is called the **leading coefficient vector** of $v(D)$, denoted by v^{lc}.

Row reduced encoders

$G(D) \in \mathbb{F}[D]^{k\times n}$ is row reduced if the *leading row coefficient matrix* G_{lrc}, whose rows are the leading coefficients vectors of the rows of $G(D)$ is full row rank.

Row reduced encoders are the ones that have minimal sum of the row degrees among all encoders of $\mathcal{C}$ $\rightarrow$ degree of $\mathcal{C}$.

If $\mathcal{C}$ has rate k/n and degree δ is said to be an (n, k, δ)-convolutional code.

Row reduced encoders

$G(D) \in \mathbb{F}[D]^{k \times n}$ is row reduced if the *leading row coefficient matrix* G_{lrc}, whose rows are the leading coefficients vectors of the rows of $G(D)$ is full row rank.

Row reduced encoders are the ones that have minimal sum of the row degrees among all encoders of $\mathcal{C}$ $\rightarrow$ degree of $\mathcal{C}$.

If $\mathcal{C}$ has rate k/n and degree δ is said to be an (n, k, δ)-convolutional code.

$\rightarrow$ δ is the minimal dimension of a realization of $\mathcal{C}$.

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

$$d(\mathcal{C}) = min\{wt(v(D)) : \ v(D) \in \mathcal{C}, \ v(D) \neq 0\},$$

where $wt(v(D))$ is the **weight** of a polynomial vector

$$v(D) = \sum_{i \geq 0} v_i D^i \in \mathbb{F}^n[D]$$

given by

$$wt(v(D)) = \sum_{i \geq 0} wt(v_i),$$

with $wt(v_i)$ the number of nonzero elements of v_i.

Singleton bound

Theorem ([1])

Let $\mathcal{C}$ be an (n, k, δ)-convolutional code. Then

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

[1] J. Rosenthal and R. Smarandache (1999)
Maximum distance separable convolutional codes
Appl. Algebra Engrg. Comm. Comput., vol. 10, pp.1532, 1999.

Convolutional codes over $\mathbb{Z}_{p^r}$

Definition

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$.

Convolutional codes over $\mathbb{Z}_{p^r}$

Definition

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$.

- Why to consider codes over finite rings? $\rightarrow$ motivated for use with phase modulation.

In particular, convolutional codes over the ring $\mathbb{Z}_M$ are useful for M-ary phase modulation (with M a positive integer). By the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$, where p is a prime integer and r is a positive integer, can be extended to codes over $\mathbb{Z}_M$.

Convolutional codes over $\mathbb{Z}_{p^r}$

Definition

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$.

Convolutional codes over $\mathbb{Z}_{p^r}$

Definition

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$.

- The theory of convolutional codes over finite rings was initiated by Massey and Mittelholzer (1990)
- Structural properties on these convolutional codes have been studied by Johannesson, Wan and Wittenmark (1998).
- Kuijper and P. introduced p-encoder and characterized the minimal p-encoders of these codes (2009).
- El Oued and Solé studied distance properties and constructed codes with optimal distance, restricted to free ones (2013).
- Napp, P. and Toste studied the column distance and obtained codes with optimal column distances (2016)

What is the main difference when we work over **rings**?

Zero divisors!

Example
Let $\mathcal{C} = \text{span}\{g_0, g_1\} \subset \mathbb{Z}_{3^3}[D]^3$ be a convolutional code, with $g_0 = [\ 1 \quad 1+D \quad 0\ ]$ and $g_1 = [\ 3 \quad 0 \quad 3+3D\ ]$.

* **Encoder** $\longrightarrow \quad \tilde{G}(D) = \begin{bmatrix} 1 & 1+D & 0 \\ 3 & 0 & 3+3D \end{bmatrix}$
* g_0, g_1 are not linearly independent!

Two messages: $u(D) = [\ 1 \quad 9\ ]$ and $\hat{u}(D) = [\ 1 \quad 0\ ]$ produce the same codeword:

$$v(D) = [\ 1 \quad 1+D \quad 0\ ].$$

In order to solve this problem we will restrict to linear combinations with coefficients in $\mathcal{A}_p[D]$ where

$$\mathcal{A}_p = \{0, 1, 2, \dots, p-1\} \subset \mathbb{Z}_{p^r}.$$

$$\downarrow$$

Any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as

$$a = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1}, \ \ \alpha_i \in \mathcal{A}_p.$$

Back to example ($\mathcal{A}_3 = \{0, 1, 2\}$)

encoder

$$\tilde{G}(D) = \begin{bmatrix} 1 & 1+D & 0 \\ 3 & 0 & 3+3D \end{bmatrix}$$

new type of encoder

$$G(D) = \begin{bmatrix} g_0 \\ 3g_0 \\ 9g_0 \\ g_1 \\ 3g_1 \end{bmatrix} = \begin{bmatrix} 1 & 1+D & 0 \\ 3 & 3+D & 0 \\ 9 & 9+9D & 0 \\ 3 & 0 & 3+3D \\ 9 & 0 & 9+9D \end{bmatrix}$$

with $u(D) \in \mathcal{A}_3[D]^5$.
Only the message $u(D) = [1\ 0\ 0\ 0\ 0] \in \mathcal{A}_3[D]^5$ produces the codeword $[1 \;\; 1+D \;\; 0]$.

$$\mathcal{A}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$$

Let $\{v_1(D), \ldots, v_k(D)\} \subset \mathbb{Z}_{p^r}^n[D]$.

$$\sum_{j=1}^{k} a_j(D)v_j(D),\ a_j(D) \in \mathcal{A}_p[D],$$

is said to be a **p-linear combination** of $v_1(D), \ldots, v_k(D)$.

The set of all p-linear combination of $v_1(D), \ldots, v_k(D)$ is called the **p-span** of $\{v_1(D), \ldots, v_k(D)\}$:

$$p\text{-span } (v_1(D), \ldots, v_k(D)).$$

Obviously, p-span $(v_1(D), \ldots, v_k(D))$ is not always a module!

The set of all p-linear combination of $v_1(D), \ldots, v_k(D)$ is called the **p-span** of $\{v_1(D), \ldots, v_k(D)\}$:

$$p\text{-span } (v_1(D), \ldots, v_k(D)).$$

Obviously, p-span $(v_1(D), \ldots, v_k(D))$ is not always a module!

Example: In $\mathbb{Z}^3_{3^3}[D]$, $p - \text{span}([1 \;\; 1+D \;\; 0])$ is not a submodule of $\mathbb{Z}^3_{3^3}[D]$.

An ordered sequence of vectors $(v_1(D), \ldots, v_k(D))$ in $\mathbb{Z}_{p^r}^n[D]$ is said to be a **p-generator sequence** if:

1. $p\, v_i(D)$ is a p-linear combination of $v_{i+1}(D), \ldots, v_k(D)$, $i = 1, \ldots, k-1$;
2. $p\, v_k(D) = 0$.

An ordered sequence of vectors $(v_1(D), \ldots, v_k(D))$ in $\mathbb{Z}_{p^r}^n[D]$ is said to be a **p-generator sequence** if:

1. $p\, v_i(D)$ is a p-linear combination of $v_{i+1}(D), \ldots, v_k(D)$, $i = 1, \ldots, k-1$;
2. $p\, v_k(D) = 0$.

Example: in $\mathbb{Z}_{3^3}^3[D]$

$$([1 \;\; 1+D \;\; 0], [3 \;\; 3+3D \;\; 0], [9 \;\; 9+9D \;\; 0])$$

is a p-generator sequence

If $V = (v_1(D), \ldots, v_k(D))$ is a p-generator sequence then

$$p\text{-}span\, V = span\, V.$$

$\rightarrow$ p-span V is a submodule of $\mathbb{Z}_{p^r}^n[D]$, and we say that V is a p-generator sequence of $M = p$-span V.

If $V = (v_1(D), \ldots, v_k(D))$ is a p-generator sequence then

$$p\text{-}span\, V = span\, V.$$

$\rightarrow$ p-span V is a submodule of $\mathbb{Z}_{p^r}^n[D]$, and we say that V is a p-generator sequence of $M = p$-span V.

If $M = span(v_1(D), \ldots, v_k(D))$ is a submodule of $\mathbb{Z}_{p^r}^n[D]$ then

$$(v_1(D), pv_1(D) \ldots, p^{r-1} v_1(D), v_2(D), pv_2(D), \ldots,$$
$$\ldots, p^{r-1} v_2(D), \ldots, v_k(D), pv_k(D) \ldots, p^{r-1} v_k(D)).$$

is a p-generator sequence of M.

The vectors $v_1(D), \ldots, v_k(D)$ are said to be **p-linearly independent** if the only p-linear combination of $v_1(D), \ldots, v_k(D)$ that is equal to 0 is the trivial one.

The vectors $v_1(D), \ldots, v_k(D)$ are said to be **p-linearly independent** if the only p-linear combination of $v_1(D), \ldots, v_k(D)$ that is equal to 0 is the trivial one.

An ordered sequence of vectors $V = (v_1(D), \ldots, v_k(D))$ which is a p-linearly independent p-generator sequence is said to be a **p-basis** and we say that V is a p-basis of $M = p$-span V.

Lemma

Two p-bases of a submodule of $\mathbb{Z}_{p^r}^n[D]$ have the same number of elements.

The number of elements of a p-basis of a submodule M of $\mathbb{Z}_{p^r}^n[D]$ is called **p-dimension** of M, denoted as $p\text{-}dim(M)$.

Example: M=span$([1 \;\; 1+D \;\; 0], [3 \;\; 0 \;\; 3+3D]) \subset \mathbb{Z}_{3^3}^3[D]$

$([1 \;\; 1{+}D \;\; 0], [3 \;\; 3{+}3D \;\; 0], [9 \;\; 9{+}9D \;\; 0], [3 \;\; 0 \;\; 3{+}3D], [9 \;\; 0 \;\; 9{+}9D])$

is a p-basis of M and consequently $p\text{-dim}(M) = 5$.

A reduced p-basis

Let $v(D)$ be a nonzero vector in $\mathbb{Z}_{p^r}^n[D]$:

$$v(D) = v_0 + v_1 D + \cdots + v_\nu D^\nu,$$

with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, \ldots, \nu$, and $v_\nu \neq 0$.

- $v(D)$ has **degree** ν, *deg* $v(D) = \nu$;
- v_ν is called the **leading coefficient vector** of $v(D)$, denoted by v^{lc}.

Let M be a submodule of $\mathbb{Z}_{p^r}^n[D]$ written as the p-span of a p-generator sequence $V = (v_1(D), \ldots, v_k(D))$.
V is called a **reduced p-basis** for M if the leading coefficient vectors $v_1^{lc}, \ldots, v_k^{lc}$ are p-linearly independent.

Example: M=span$([1\ \ 1+D\ \ 0], [3\ \ 0\ \ 3+3D]) \subset \mathbb{Z}_{3^3}^3[D]$

$([1\ \ 1{+}D\ \ 0], [3\ \ 3{+}3D\ \ 0], [9\ \ 9{+}9D\ \ 0], [3\ \ 0\ \ 3{+}3D], [9\ \ 0\ \ 9{+}9D])$

is a reduced p-basis of M since the leading coefficient vectors

$$([0\ \ 1\ \ 0], [\ \ 3\ \ 0], [0\ \ 9\ \ 0], [0\ \ 0\ \ 3], [0\ \ 0\ \ 9])$$

are p-linearly independent.

Every submodule M of $\mathbb{Z}_{p^r}^n[D]$ has a reduced p-basis.

The sum of the degrees of a reduced p-basis of M is minimal among all the p-bases of M $\rightarrow$ p-degree of M.

Convolutional codes over $\mathbb{Z}_{p^r}$

A **convolutional code** $\mathcal{C}$ of length n is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$. If $\mathcal{C}$ has p-dimension k and p-degree δ, we say that $\mathcal{C}$ is an (n, k, δ)-convolutional code.

Convolutional codes over $\mathbb{Z}_{p^r}$

A **convolutional code** $\mathcal{C}$ of length n is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$. If $\mathcal{C}$ has p-dimension k and p-degree δ, we say that $\mathcal{C}$ is an (n, k, δ)-convolutional code.

A **p-encoder** $G(D) \in \mathbb{Z}_{p^r}[D]^{k \times n}$ of $\mathcal{C}$ is a polynomial matrix whose rows are a p-basis of $\mathcal{C}$ and therefore

$$\mathcal{C} = Im_{\mathcal{A}_p[D]} G(D) = \left\{ u(D)G(D) \in \mathbb{Z}_{p^r}^n[D] : \; u(D) \in \mathcal{A}_p[D]^k \right\}.$$

M. Kuijper, R. Pinto and J.W.Polderman (2007)
The predictable degree property and row reducedness for systems over a finite ring
Linear Alg. Appl., Vol. 425, pp. 776-796, 2007.

M. Kuijper, R. Pinto (2009)
On minimality of convolutional ring encoders
IEEE Trans. Information Theory, Vol. 55, No. 11, pp. 4890-4897, November 2009.

Free Distance

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

$$d(\mathcal{C}) = min\{wt(v(D)) : \ v(D) \in \mathcal{C}, \ v(D) \neq 0\},$$

where $wt(v(D))$ is the **weight** of a polynomial vector

$$v(D) = \sum_{i \geq 0} v_i D^i \in \mathbb{Z}_{p^r}^n[D]$$

given by

$$wt(v(D)) = \sum_{i \geq 0} wt(v_i),$$

with $wt(v_i)$ the number of non zero elements of v_i.

Theorem

The free distance of an (n, k, δ)-convolutional code $\mathcal{C}$ satisfies

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

M. El Oued and P. Solé (2013)
MDS Convolutional Codes Over a Finite Ring
IEEE trans. info. theory, Vol. 59, n. 11, november 2013.

D. Napp, R. Pinto and M. Toste
On MDS Convolutional Codes Over $\mathbb{Z}_{p^r}$
accepted in Designs, Codes and Cryptography.

An (n, k, δ)-convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is said to be **Maximum Distance Separable** (MDS) if

$$d(\mathcal{C}) = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1.$$

Constructions of MDS convolutional codes [1]

Given $n, k, \delta \in \mathbb{N}$, let us construct an MDS (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$.

For simplicity, assume that $\mathbf{k} \mid \boldsymbol{\delta}$.
Determine $(k_0, k_1, \ldots, k_{r-1})$ such that

$$\begin{aligned} k_0 + k_1 + \cdots + k_{r-1} &= \min_{k = rk_0' + (r-1)k_1' + \cdots + k_{r-1}'} (k_0' + k_1' + \cdots + k_{r-1}') \\ &= \left\lceil \frac{k}{r} \right\rceil . \end{aligned}$$

[1] D. Napp, R. Pinto, M. Toste (2016)
On MDS convolutional codes over Z_p^r
Designs Codes and Cryptography, 83(1), 101-104.

Consider an MDS $(\tilde{n}, \tilde{k}, \tilde{\delta})$-convolutional codes $\widetilde{\mathcal{C}}$ over the field $\mathbb{Z}_p$ [1] with

$$\widetilde{n} = n,$$

$$\widetilde{k} = k_0 + k_1 + \cdots + k_{r-1} = \left\lceil \frac{k}{r} \right\rceil,$$

$$\widetilde{\delta} = \frac{\delta}{k}\widetilde{k}.$$

[1] Smarandache, R. and Gluesing-Luerssen, H. and Rosenthal, J. (2001)
Constructions for MDS-Convolutional Codes
IEEE Trans. Automat. Control, vol. 47-5, pp.2045-2049, 2001.

Let

$$\widetilde{G}(D) = \begin{bmatrix} \widetilde{G}_{k_0}(D) \\ ----- \\ \widetilde{G}_{k_1}(D) \\ ----- \\ \vdots \\ ----- \\ \widetilde{G}_{k_{r-1}}(D) \end{bmatrix} \in \mathbb{Z}_p[D]^{\widetilde{k} \times n}$$

be an encoder of $\widetilde{\mathcal{C}}$ in reduced form, where $\widetilde{G}_{k_i}(D)$ is a $k_i \times n$ matrix, $i = 0, 1, \dots, r-1$, .

The distance of $\widetilde{\mathcal{C}}$ equals

$$d(\widetilde{\mathcal{C}}) = (n - \widetilde{k}) \left(\left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + 1 \right) + \widetilde{\delta} + 1.$$

From $\widetilde{k} = \left\lceil \frac{k}{r} \right\rceil$ and $\widetilde{\delta} = \frac{\delta}{k} \widetilde{k}$ we get that

$$\begin{aligned} d(\widetilde{\mathcal{C}}) &= n \left(\frac{\delta}{k} + 1 \right) - \left\lceil \frac{k}{r} \right\rceil + 1 \\ &= n \left(\frac{\delta}{k} + 1 \right) - \left\lceil \frac{k}{r} \left(\frac{\delta}{k} + 1 \right) - \frac{\delta}{r} \right\rceil + 1 \end{aligned}$$

We *lift* $\widetilde{G}(D)$ to construct a $k \times n$ matrix $G(D)$:

$$G(D) = \begin{bmatrix} \widetilde{G}_{k_0}(D) \\ p\widetilde{G}_{k_0}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_0}(D) \\ --\,-- \\ p\widetilde{G}_{k_1}(D) \\ p^2\widetilde{G}_{k_1}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_1}(D) \\ --\,-- \\ \vdots \\ --\,-- \\ p^{r-1}\widetilde{G}_{k_{r-1}}(D) \end{bmatrix} \in \mathbb{Z}_{p^r}^{k\times n}[D].$$

Theorem

The matrix $G(D)$ defined above is a reduced p-encoder of an (n, k, δ)-convolutional code $\mathcal{C}$ with $k \mid \delta$. Moreover, $\mathcal{C}$ is MDS, *i.e.*,

$$d(\mathcal{C}) = n\left(\frac{\delta}{k}+1\right) - \left\lceil \frac{k}{r}\left(\frac{\delta}{k}+1\right) - \frac{\delta}{r} \right\rceil + 1$$

Remarks

- The constructions of MDS convolutional codes over $\mathbb{Z}_{p^r}$ are "based" on MDS convolutional codes over $\mathbb{Z}_p$.
- The known constructions of a (n, k, δ)- convolutional code require very large fields.
- Open problem: construct MDS convolutional codes for fields of small size.

Remarks

- Another important distance measure of a convolutional code is the column distance:

$$d_j^c(\mathcal{C}) = \min\{wt(v_{[0,j]}) : v_0 \neq 0\}$$

Convolutional codes whose column distances increase as maximum as possible for as long as possible are called Maximum Distance Profile (MDP) codes $\rightarrow$ appealing for sequential decoding algorithms.

D. Napp, R. Pinto, M. Toste
Column distance of convolutional codes over Z_{p^r}
submitted (available in arXiv)

Dual code

$$\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{p^r}[D]} G(D) \subset \tilde{\mathcal{C}} = Im_{\mathbb{Z}_{p^r}((D))} G(D)$$

Dual code

$$\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{p^r}[D]} G(D) \subset \tilde{\mathcal{C}} = Im_{\mathbb{Z}_{p^r}((D))} G(D)$$

Definition

A convolutional code over $\mathbb{Z}_{p^r}((D))$ is a $\mathbb{Z}_{p^r}((D))$-submodule of $\mathbb{Z}_{p^r}^n((D))$ for which there exists a polynomial matrix $G(D) \in \mathbb{Z}_{p^r}^{\hat{k}\times n}[D]$ such that

$$\begin{aligned} \mathcal{C} &= \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} G(D) \\ &= \{u(D)G(D) \in \mathbb{Z}_{p^r}^n((D)) : u(D) \in \mathbb{Z}_{p^r}^{\hat{k}}((D))\} \end{aligned}$$

$G(D)$ is called a generator matrix. If $G(D)$ is full row rank it is called an encoder and $\mathcal{C}$ is free.

Dual code

Definition

Let $\mathcal{C}$ be a convolutional code over $\mathbb{Z}_{p^r}((D))$. The dual of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp} = \{y(D) \in \mathbb{Z}_{p^r}^{n}((D)) : y(D)v(D)^{T} = 0 \quad \forall v(D) \in \mathcal{C}\}$$

Dual of a free convolutional code

Let $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} G(D)$ be a free convolutional code with $G(D) \in \mathbb{Z}_{p^r}^{\hat{k} \times n}[D]$ full row rank

There exists $N(D) \in \mathbb{Z}_{p^r}^{(n-\hat{k}) \times n}((D))$ such that $\begin{bmatrix} G(D) \\ N(D) \end{bmatrix}$ is invertible

$$\mathbb{Z}_{p^r}[D] \subset \mathbb{Z}_{p^r}(D) \subset \mathbb{Z}_{p^r}((D))$$

$\mathbb{Z}_{p^r}(D)$: ring of rational matrices

$$\mathbb{Z}_{p^r}(D) = \left\{ \frac{p(D)}{q(D)} : p(D), q(D) \in \mathbb{Z}_{p^r}[D] \text{ and the coefficient of the smallest power of } D \text{ in } q(D) \text{ is a unit} \right\}$$

Let $L(D) \in \mathbb{Z}_{p^r}^{n\times \hat{k}}(D)$ and $\tilde{H}(D) \in \mathbb{Z}_{p^r}^{n\times (n-\hat{k})}(D)$ such that

$$\begin{bmatrix} G(D) \\ N(D) \end{bmatrix} \begin{bmatrix} L(D) & \tilde{H}(D) \end{bmatrix} = I$$

Let $L(D) \in \mathbb{Z}_{p^r}^{n\times\hat{k}}(D)$ and $\tilde{H}(D) \in \mathbb{Z}_{p^r}^{n\times(n-\hat{k})}(D)$ such that

$$\begin{bmatrix} G(D) \\ N(D) \end{bmatrix} \begin{bmatrix} L(D) & \tilde{H}(D) \end{bmatrix} = I$$

$$v(D) \in \mathcal{C} \;\Leftrightarrow\; v(D)\tilde{H}(D) = 0$$

$$\mathcal{C}^{\perp} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))}\,\tilde{H}(D) = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))}\,H(D)$$

for some $H(D) \in \mathbb{Z}_{p^r}^{n\times(n-\hat{k})}[D]$ full row rank

Remark: The parity-check matrices of $\mathcal{C}$ are the transposes of the encoders of $\mathcal{C}^{\perp}$ and $\mathcal{C}^{\perp}$ is a convolutional code of rate $(n-\hat{k})/n$

Example

In $\mathbb{Z}_{3^2}$; $n = 3$, $\hat{k} = 2$

$$G(D) = \left[\begin{array}{ccc} 1 + D & 1 & 3D \\ 0 & 1 + D & 1 + D \end{array} \right]$$

full row rank. $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))}\, G(D)$ free convolutional code

Example

In $\mathbb{Z}_{3^2}$; $n = 3$, $\hat{k} = 2$

$$G(D) = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \end{bmatrix}$$

full row rank. $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))}\, G(D)$ free convolutional code

$$\begin{bmatrix} G(D) \\ N(D) \end{bmatrix} = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix}$$

invertible

Inverse of $\begin{bmatrix} G(D) \\ N(D) \end{bmatrix}$:

$$\begin{bmatrix} L(D) & \tilde{H}(D) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ \frac{1+D}{1+7D+6D^2} & \frac{6D}{1+7D+6D^2} & \frac{8+7D+8D^2}{1+7D+6D^2} \\ \frac{8+8D}{1+7D+6D^2} & \frac{1}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix}$$

$H(D) = \begin{bmatrix} 1+7D+6D^2 \\ 8+7D+8D^2 \\ 1+2D+D^2 \end{bmatrix}$ is a parity-check matrix of $\mathcal{C}$ and

$$\mathcal{C}^\perp = Im_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \end{bmatrix}$$

General convolutional codes

General convolutional codes

Theorem

Let $\mathcal{C}$ be a convolutional code over $\mathbb{Z}_{p^r}((D))$. Then there exist $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{r-1}$ free convolutional codes such that

$$\mathcal{C} = \mathcal{C}_0 \oplus p\,\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\,\mathcal{C}_{r-1}$$

with

$$\mathcal{C}_0 + \mathcal{C}_1 + \cdots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1}.$$

From a generator matrix $G(D)$ of $\mathcal{C}$ $\rightsquigarrow$

$\rightsquigarrow$ build another generator matrix $\tilde{G}(D) = \begin{bmatrix} G_0(D) \\ p\,G_1(D) \\ \vdots \\ p^{r-1}\,G_{r-1}(D) \end{bmatrix}$

such that $\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}$ is full row rank

M. El Oued, D. Napp, R. Pinto and M. Toste (2015)
The dual of convolutional codes over $\mathbb{Z}_{p^r}$
Applied and Computational Matrix Analysis Algebra Engrg. Comm. Comput., vol. 10, pp.7991, 2015.

Theorem

Let $\mathcal{C}$ *be a convolutional code over* $\mathbb{Z}_{p^r}((D))$ *and* $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{r-1}$ *free convolutional codes such that*

$$\mathcal{C} = \mathcal{C}_0 \oplus p\,\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\,\mathcal{C}_{r-1}$$

with

$$\mathcal{C}_0 + \mathcal{C}_1 + \cdots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1}$$

and let

$$B_0 = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^{\perp}$$

and $B_{r-i},\ i = 1, \ldots, r-1$ *such that*

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1} \oplus \mathcal{C}_i)^{\perp} \oplus B_{r-i}.$$

Then

$$\mathcal{C}^{\perp} = B_0 \oplus p\,B_1 \oplus \cdots \oplus p^{r-1}\,B_{r-1}.$$

Example

In $\mathbb{Z}_{3^2}$. Let us consider $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} G(D)$ where

$$G(D) = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 3+3D & 3+3D \end{bmatrix}$$

Example

In $\mathbb{Z}_{3^2}$. Let us consider $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} G(D)$ where

$$G(D) = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 3+3D & 3+3D \end{bmatrix}$$

$\mathcal{C} = \mathcal{C}_0 \oplus 3\mathcal{C}_1$ with

$$\mathcal{C}_0 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+D & 1 & 3D \end{bmatrix}$$

and

$$\mathcal{C}_1 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 0 & 1+D & 1+D \end{bmatrix}$$

such that

$$\mathcal{C}_0 \oplus \mathcal{C}_1 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \end{bmatrix}$$

Example

In $\mathbb{Z}_{3^2}$. Let us consider $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} G(D)$ where

$$G(D) = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 3+3D & 3+3D \end{bmatrix}$$

$\mathcal{C} = \mathcal{C}_0 \oplus 3\mathcal{C}_1$ with

$$\mathcal{C}_0 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+D & 1 & 3D \end{bmatrix}$$

and

$$\mathcal{C}_1 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 0 & 1+D & 1+D \end{bmatrix}$$

such that

$$\mathcal{C}_0 \oplus \mathcal{C}_1 = \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \end{bmatrix}$$

Dual of $\mathcal{C}$: $\mathcal{C}^{\perp} = B_0 \oplus 3B_1$ where

$$\begin{aligned} B_0 &= (\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \\ &= \mathrm{Im}_{\mathbb{Z}_{3^2}((D))} \left[\begin{array}{ccc} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \end{array} \right] \end{aligned}$$

B_1 is such that $\mathcal{C}_0^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \oplus B_1$

$$\begin{bmatrix} G(D) \\ N(D) \end{bmatrix} = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix}$$

To determine B_0

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ \frac{1+D}{1+7D+6D^2} & \frac{6D}{1+7D+6D^2} & \frac{8+7D+8D^2}{1+7D+6D^2} \\ \frac{8+8D}{1+7D+6D^2} & \frac{1}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix} = I$$

$$B_0 = Im_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \end{bmatrix}$$

To determine B_1 $\left(\mathcal{C}_0^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \oplus B_1\right)$

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ \frac{1+D}{1+7D+6D^2} & \frac{6D}{1+7D+6D^2} & \frac{8+7D+8D^2}{1+7D+6D^2} \\ \frac{8+8D}{1+7D+6D^2} & \frac{1}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix} = I$$

$$B_1 = \mathrm{Im}_{Z_{3^2}((D))} \left[\begin{array}{ccc} 0 & 6D & 1 \end{array} \right]$$

To determine B_1 $\left(\mathcal{C}_0^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \oplus B_1\right)$

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ \frac{1+D}{1+7D+6D^2} & \frac{6D}{1+7D+6D^2} & \frac{8+7D+8D^2}{1+7D+6D^2} \\ \frac{8+8D}{1+7D+6D^2} & \frac{1}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix} = I$$

$$B_1 = \mathrm{Im}_{Z_{3^2}((D))} \left[\begin{array}{ccc} 0 & 6D & 1 \end{array}\right]$$

$$\mathcal{C}^{\perp} = Im_{\mathbb{Z}_{3^2}((D))} \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \\ 0 & 0 & 3 \end{bmatrix}$$

Thank you for your attention!