Course on (algebraic aspects of) Convolutional Codes

Diego Napp

Department of Mathematics, Universidad of Aveiro, Portugal

CIDMA CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

CIMPA RESEARCH SCHOOL

July 11, 2017

My most heartfelt thanks to the organizers

CIMPA RESEARCH SCHOOL

ALGEBRAIC METHODS IN CODING THEORY

Overview

1. Error-correcting codes: From block codes to convolutional codes
   - Basics: Polynomial encoders
2. Distance properties of convolutional codes
   - Maximum Distance Profile (MDP) and Maximum Distance Separable (MDS)
   - Construction of MDP and MDS: Superregular matrices
3. Decoding of Convolutional codes
   - Viterbi algorithm
   - Decoding of convolutional codes over the erasure channel
4. Network coding with convolutional codes
5. Avenues for further research
   - Motivated by applications: Video streaming and storage systems
   - More theoretical: Multidimensional convolutional codes and convolutional codes over $\mathbb{Z}_{p^r}$

Day 5: 2D Convolutional Codes

- One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction.

Day 5: 2D Convolutional Codes

- One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction.
- To encode data recorded geometrically in m dimensions (mD, with $m > 1$), e.g., pictures or videos.

Day 5: 2D Convolutional Codes

- One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction.
- To encode data recorded geometrically in m dimensions (mD, with $m > 1$), e.g., pictures or videos.
- It is possible to work in a framework that takes advantage of the correlation of the data in several directions.

Day 5: 2D Convolutional Codes

- One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction.
- To encode data recorded geometrically in m dimensions (mD, with $m > 1$), e.g., pictures or videos.
- It is possible to work in a framework that takes advantage of the correlation of the data in several directions.
- Such framework would lead to m dimensional (mD) convolutional codes, generalizing the notion of 1D convolutional code.

Day 5: 2D Convolutional Codes

- One dimensional (1D) convolutional codes are very much suited for encoding data recorded in one single direction.
- To encode data recorded geometrically in m dimensions (mD, with $m > 1$), e.g., pictures or videos.
- It is possible to work in a framework that takes advantage of the correlation of the data in several directions.
- Such framework would lead to m dimensional (mD) convolutional codes, generalizing the notion of 1D convolutional code.
- This generalization is nontrivial since 1D convolutional codes are represented over the polynomial ring in one variable whereas mD convolutional codes are represented over the polynomial ring in m independent variables.

Basics for 2D Convolutional Codes

- Many fundamental issues such as error correction capability, decoding algorithms, etc., that are well known for 1D convolutional codes have not been sufficiently investigated in the context of mD convolutional codes.

Basics for 2D Convolutional Codes

- Many fundamental issues such as error correction capability, decoding algorithms, etc., that are well known for 1D convolutional codes have not been sufficiently investigated in the context of mD convolutional codes.
- The first attempts to develop the general theory and the basic algebraic properties of 2D/mD convolutional codes were proposed in some papers. Questions about optimal distances and constructions of codes with large distance remained wide open for many years

Basics for 2D Convolutional Codes

- Many fundamental issues such as error correction capability, decoding algorithms, etc., that are well known for 1D convolutional codes have not been sufficiently investigated in the context of mD convolutional codes.
- The first attempts to develop the general theory and the basic algebraic properties of 2D/mD convolutional codes were proposed in some papers. Questions about optimal distances and constructions of codes with large distance remained wide open for many years
- Next we introduce the basic notions of 2D convolutional codes that, despite its fundamental importance, have been very little investigated.

Basics for 2D Convolutional Codes

Definition

Let $\mathbb{F}$ be a finite field and $\mathbb{F}[z_1, z_2]$ the ring of polynomials in two variables with coefficients in $\mathbb{F}$.

Basics for 2D Convolutional Codes

Definition

Let $\mathbb{F}$ be a finite field and $\mathbb{F}[z_1, z_2]$ the ring of polynomials in two variables with coefficients in $\mathbb{F}$. A 2D convolutional code $\mathcal{C}$ of rate k/n is a free $\mathbb{F}[z_1, z_2]$- submodule of $\mathbb{F}[z_1, z_2]^n$, where k is the rank of $\mathcal{C}$.

Basics for 2D Convolutional Codes

Definition

Let $\mathbb{F}$ be a finite field and $\mathbb{F}[z_1, z_2]$ the ring of polynomials in two variables with coefficients in $\mathbb{F}$. A 2D convolutional code $\mathcal{C}$ of rate k/n is a free $\mathbb{F}[z_1, z_2]$- submodule of $\mathbb{F}[z_1, z_2]^n$, where k is the rank of $\mathcal{C}$.

Definition

A full row rank matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ whose rows constitute a basis for $\mathcal{C}$ is called a generator matrix or encoder of $\mathcal{C}$.

Definition

A matrix $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times n}$ is *unimodular* if it has a polynomial inverse ou equivalently if $\det U(z_1, z_2) \in \mathbb{F}\backslash\{0\}$.

Definition

A matrix $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times n}$ is *unimodular* if it has a polynomial inverse ou equivalently if $\det U(z_1, z_2) \in \mathbb{F}\backslash\{0\}$.
A matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$, with $n \geq k$, is called *left factor prime* (lFP) if for every factorization $G(z_1, z_2) = \bar{V}(z_1, z_2)G(z_1, z_2)$, with $V(z_1, z_2) \in \mathbb{F}^{k\times k}$, $V(z_1, z_2)$ is unimodular.

Definition

A matrix $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n \times n}$ is *unimodular* if it has a polynomial inverse ou equivalently if $\det U(z_1, z_2) \in \mathbb{F} \backslash \{0\}$.
A matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$, with $n \geq k$, is called *left factor prime* (lFP) if for every factorization $G(z_1, z_2) = \bar{V}(z_1, z_2) G(z_1, z_2)$, with $V(z_1, z_2) \in \mathbb{F}^{k \times k}$, $V(z_1, z_2)$ is unimodular.
And it is called *left zero prime* (lZP) if $G(z_1, z_2)$ admits a polynomial left inverse.

Theorem

Let $G(z_1, z_2) \in \mathbb{F}^{n\times k}$, with $n \geq k$. Then the following are equivalent:

i) $G(z_1, z_2)$ is left factor prime;

ii) there exists polynomial matrices $X_i(z_1, z_2)$ such that $G(z_1, z_2)X_i(z_1, z_2) = d_i(z_i)I_k$, where $d_i(z_i) \in \mathbb{F}[z_i]\backslash\{0\}$, for $i = 1, 2$;

Theorem

Let $G(z_1, z_2) \in \mathbb{F}^{n\times k}$, with $n \geq k$. Then the following are equivalent:

i) $G(z_1, z_2)$ is left factor prime;

ii) there exists polynomial matrices $X_i(z_1, z_2)$ such that $G(z_1, z_2)X_i(z_1, z_2) = d_i(z_i)I_k$, where $d_i(z_i) \in \mathbb{F}[z_i]\backslash\{0\}$, for $i = 1, 2$;

Theorem

i) $G(z_1, z_2)$ is right zero prime;

ii) $G(z_1, z_2)$ admits a polynomial left inverse;

iii) there exists a polynomial matrix $V(z_1, z_2) \in \mathbb{F}^{n\times(n-k)}$ such that $[G(z_1, z_2) \;\; V(z_1, z_2)]$ is unimodular.

Theorem

Let $G(z_1, z_2) \in \mathbb{F}^{n \times k}$, with $n \geq k$. Then the following are equivalent:

i) $G(z_1, z_2)$ is left factor prime;

ii) there exists polynomial matrices $X_i(z_1, z_2)$ such that $G(z_1, z_2)X_i(z_1, z_2) = d_i(z_i)I_k$, where $d_i(z_i) \in \mathbb{F}[z_i]\backslash\{0\}$, for $i = 1, 2$;

Theorem

i) $G(z_1, z_2)$ is right zero prime;

ii) $G(z_1, z_2)$ admits a polynomial left inverse;

iii) there exists a polynomial matrix $V(z_1, z_2) \in \mathbb{F}^{n \times (n-k)}$ such that $[G(z_1, z_2) \;\; V(z_1, z_2)]$ is unimodular.

It follows that zero primeness implies factor primeness, but the converse is not true.

References

E. Fornasini and M. E. Valcher.
Algebraic aspects of two-dimensional convolutional codes.
IEEE Transactions on Information Theory, **40(4)**: 1068–1082 (1994).

E. Fornasini and M. E. Valcher.
Multidimensional systems with finite support behaviors: Signal structure, generation, and detection.
SIAM Journal on Control and Optimization, **36(2)**: 760–779 (1998).

P. A. Weiner.
Multidimensional Convolutional Codes.
PhD thesis, Department of Mathematics, University of Notre Dame, Indiana, USA, April 1998.

D. Napp, C. Perea, and R. Pinto.
Input-state-output representations and constructions of finite support 2D convolutional codes.
Advances in Mathematics of Communications, **4(4)**: 533–545 (2010).

Cem Gneri ; Buket zkaya.
Multidimensional Quasi-Cyclic and Convolutional Codes
IEEE Transactions on Information Theory , **62(12)**: 6772–6785 (2016).

Basics for 2D Convolutional Codes

Lemma

Two generator matrices $G_1(z_1, z_2), G_2(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ define the same 2D convolutional code $\mathcal{C}$ if and only if there exists $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times k}$, unimodular, such that

$$G_2(z_1, z_2) = U(z_1, z_2) G_1(z_1, z_2)$$

Basics for 2D Convolutional Codes

Lemma

Two generator matrices $G_1(z_1, z_2), G_2(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ define the same 2D convolutional code $\mathcal{C}$ if and only if there exists $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times k}$, unimodular, such that

$$G_2(z_1, z_2) = U(z_1, z_2) G_1(z_1, z_2)$$

Definition

The degree δ of a 2D convolutional code $\mathcal{C}$ is the maximum of the degrees of the determinants of the $k \times k$ submatrices of any generator matrix of $\mathcal{C}$.

Minimal realization of 1D convolutional codes are very useful for many reasons: less amount of memory, help to construction of good codes, etc. These state-space representations are obtained via realizations of the encoders of the code. We know how to characterize them.

Minimal realization of 1D convolutional codes are very useful for many reasons: less amount of memory, help to construction of good codes, etc. These state-space representations are obtained via realizations of the encoders of the code. We know how to characterize them.

Open problem: Minimal realizations

When considering the 2D case, there exist several state-space models (e.g. Marchesini-Fornasini or Roesser model). While in the 1D case there exists a characterization of minimality for realization via state-space models, the same does not happen in the 2D case.

Basics for 2D Convolutional Codes

Definition

The weight of $v(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} v_{(i,j)}\, z_1^i z_2^j \in \mathbb{F}[z_1, z_2]^n$ is defined as

$$\tilde{\mathbf{w}} v(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} \tilde{\mathbf{w}} v_{(i,j)}$$

Basics for 2D Convolutional Codes

Definition

The weight of $v(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} v_{(i,j)}\, z_1^i z_2^j \in \mathbb{F}[z_1, z_2]^n$ is defined as

$$\tilde{\mathbf{w}} v(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} \tilde{\mathbf{w}} v_{(i,j)}$$

Definition

The (free) distance of a 2D convolutional code $\mathcal{C}$ is defined as

$$d_{\text{free}}\mathcal{C} = \min\{\tilde{\mathbf{w}} v(z_1, z_2) \mid v(z_1, z_2) \in \mathcal{C} \setminus \{0\}\}$$

Theorem

If $\mathcal{C}$ is a 2D convolutional code of rate k/n and degree δ, then

$$d_{\text{free}}\mathcal{C} \leq \frac{(\lfloor \delta/k \rfloor + 1)(\lfloor \delta/k \rfloor + 2)}{2} n - (k - \delta + k\lfloor \delta/k \rfloor) + 1$$

Definition

A 2D convolutional code of rate k/n and degree δ with distance achieving this bound is called 2D MDS convolutional code.

A construction of a 2D convolutional code of rate 1/n

Theorem

Let $n, \delta \in \mathbb{N}$. Assume that $n \geq \ell = \frac{(\delta+1)(\delta+2)}{2}$ and consider a superregular matrix

$$G = \begin{bmatrix} G_0 & G_1 & \cdots & G_{\ell-1} \end{bmatrix} \in \mathbb{F}^{n\times\ell}.$$

Define

$$\begin{aligned} G(z_1, z_2) = G_0 + G_1 z_1 + G_2 z_2 + G_3 z_1^2 + G_4 z_1 z_2 + G_5 z_2^2 + \cdots \\ + G_{\frac{\delta(\delta+1)}{2}} z_1^{\delta} + G_{\frac{\delta(\delta+1)}{2}+1} z_1^{\delta-1} z_2 + \cdots + G_{\ell-1} z_2^{\delta}\ . \end{aligned}$$

Let $G(z_1, z_2)$ is the generator matrix of an 2D MDS convolutional code of rate $1/n$ and degree δ.

Example

In order to construct a 2D convolutional code of rate $1/12$ and $\delta = 3$ we build a superregular Cauchy matrix of size 12×10. We need a field with at least 22 elements and then we consider the field $\mathbb{F} = GF(23)$. Take for instance,

$$\vec{x} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11], \ \vec{y} = [13, 14, 15, 16, 17, 18, 19, 20, 21, 22]$$

then we obtain the Cauchy matrix

$$A = \begin{bmatrix} 7 & 18 & 3 & 10 & 4 & 14 & 6 & 8 & 12 & 1 \\ 21 & 7 & 18 & 3 & 10 & 4 & 14 & 6 & 8 & 12 \\ 2 & 21 & 7 & 18 & 3 & 10 & 4 & 14 & 6 & 8 \\ 16 & 2 & 21 & 7 & 18 & 3 & 10 & 4 & 14 & 6 \\ 5 & 16 & 2 & 21 & 7 & 18 & 3 & 10 & 4 & 14 \\ 20 & 5 & 16 & 2 & 21 & 7 & 18 & 3 & 10 & 4 \\ 13 & 20 & 5 & 16 & 2 & 21 & 7 & 18 & 3 & 10 \\ 19 & 13 & 20 & 5 & 16 & 2 & 21 & 7 & 18 & 3 \\ 9 & 19 & 13 & 20 & 5 & 16 & 2 & 21 & 7 & 18 \\ 17 & 9 & 19 & 13 & 20 & 5 & 16 & 2 & 21 & 7 \\ 15 & 17 & 9 & 19 & 13 & 20 & 5 & 16 & 2 & 21 \\ 11 & 15 & 17 & 9 & 19 & 13 & 20 & 5 & 16 & 2 \end{bmatrix}.$$

Example

Now using the theorem we have the 2D CC of rate $1/12$ and $\delta = 3$ generated by the matrix

$$\begin{bmatrix}
7 + 18z_1 + 3z_2 + 10z_1^2 + 4z_1z_2 + 14z_2^2 + 6z_1^3 + 8z_1^2z_2 + 12z_1z_2^2 + z_2^3 \\
21 + 7z_1 + 18z_2 + 3z_1^2 + 10z_1z_2 + 4z_2^2 + 14z_1^3 + 6z_1^2z_2 + 8z_1z_2^2 + 12z_2^3 \\
2 + 21z_1 + 7z_2 + 18z_1^2 + 3z_1z_2 + 10z_2^2 + 4z_1^3 + 14z_1^2z_2 + 6z_1z_2^2 + 8z_2^3 \\
16 + 2z_1 + 21z_2 + 7z_1^2 + 18z_1z_2 + 3z_2^2 + 10z_1^3 + 4z_1^2z_2 + 14z_1z_2^2 + 6z_2^3 \\
5 + 16z_1 + 2z_2 + 21z_1^2 + 7z_1z_2 + 18z_2^2 + 3z_1^3 + 10z_1^2z_2 + 4z_1z_2^2 + 14z_2^3 \\
20 + 5z_1 + 16z_2 + 2z_1^2 + 21z_1z_2 + 7z_2^2 + 18z_1^3 + 3z_1^2z_2 + 10z_1z_2^2 + 4z_2^3 \\
13 + 20z_1 + 5z_2 + 16z_1^2 + 2z_1z_2 + 21z_2^2 + 7z_1^3 + 18z_1^2z_2 + 3z_1z_2^2 + 10z_2^3 \\
19 + 13z_1 + 20z_2 + 5z_1^2 + 16z_1z_2 + 2z_2^2 + 21z_1^3 + 7z_1^2z_2 + 18z_1z_2^2 + 3z_2^3 \\
9 + 19z_1 + 13z_2 + 20z_1^2 + 5z_1z_2 + 16z_2^2 + 2z_1^3 + 21z_1^2z_2 + 7z_1z_2^2 + 18z_2^3 \\
17 + 9z_1 + 19z_2 + 13z_1^2 + 20z_1z_2 + 5z_2^2 + 16z_1^3 + 2z_1^2z_2 + 21z_1z_2^2 + 7z_2^3 \\
15 + 17z_1 + 9z_2 + 19z_1^2 + 13z_1z_2 + 20z_2^2 + 5z_1^3 + 16z_1^2z_2 + 2z_1z_2^2 + 21z_2^3 \\
11 + 15z_1 + 17z_2 + 9z_1^2 + 19z_1z_2 + 13z_2^2 + 20z_1^3 + 5z_1^2z_2 + 16z_1z_2^2 + 2z_2^3
\end{bmatrix}$$

is a 2D MDS convolutional code.

Codes over $\mathbb{Z}_{p^r}$

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

- Motivation: Convolutional codes over the ring $\mathbb{Z}_M$ are the most suitable for phase modulation signals [1].

J.L. Massey and T. Mittelholzer. (1990)
"Systematicity of convolutional codes over rings".

R. Johannesson, Z. Wan, and E. Wittenmark (1998)
Some structural properties of convolutional codes over rings
IEEE Trans. Information Theory, IT-44:839845, 1998.

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

C. Feng, R W. Nobrega, F R. Kschischang and D Silva (2014)
Communication over Finite-Chain-Ring Matrix Channels
IEEE trans. info. theory, 2014.

- Motivation: Convolutional codes over the ring $\mathbb{Z}_M$ are the most suitable for phase modulation signals [1].
- We start with the ring $\mathbb{Z}_{p^r}$. By the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$ can be extended to codes over $\mathbb{Z}_M$.

J.L. Massey and T. Mittelholzer. (1990)
"Systematicity of convolutional codes over rings".

R. Johannesson, Z. Wan, and E. Wittenmark (1998)
Some structural properties of convolutional codes over rings
IEEE Trans. Information Theory, IT-44:839845, 1998.

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

C. Feng, R W. Nobrega, F R. Kschischang and D Silva (2014)
Communication over Finite-Chain-Ring Matrix Channels
IEEE trans. info. theory, 2014.

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 $\mathbb{Z}_{p^r}^n[D]$.

Now we have to take care of the Zero divisors

Example

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

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

We only have a minimum number of generators but not necessarily linearly independent.

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

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

$$\downarrow$$

Obviously any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as (the p-adic expansion)

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

Example

Back to example

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 $u(D) \in \mathcal{A}_p[D]^5$.

Example

Back to example

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

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 $\mathbb{Z}_{p^r}[D]$-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 $\mathbb{Z}_{p^r}[D]$-module!

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

$$[3 \;\; 3+3D \;\; 0] \notin p\text{-span}([1 \;\; 1+D \;\; 0])$$

Thus 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 $(v_1(D), \dots, v_k(D))$ in $\mathbb{Z}^n_{p^r}[D]$ is said to be a **p-generator sequence** if:

1. $p\, v_i(D)$ is a p-linear combination of $v_{i+1}(D), \dots, v_k(D)$, $i = 1, \dots, k-1$;
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 $M =$span V.

If $V = (v_1(D), \dots, v_k(D))$ 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 =span V.

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

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

is a p-generator sequence of M.

Example

$M = \text{span}\{[1+D \;\; 2+2D], [9 \;\; 0], [0 \;\; 9]\} \subset \mathbb{Z}_{3^3}^3[D]$

Example

$M =$span$\{[1+D \;\; 2+2D],[9 \;\; 0],[0 \;\; 9]\} \subset \mathbb{Z}_{3^3}^3[D]$

$$([1+D \;\; 2+2D],[3+3D \;\; 6+6D],[9 \;\; 0],[0 \;\; 9])$$

is a p-generator sequence of M:

$$3[1+D \;\; 2+2D] = [3+3D \;\; 6+6D]$$

$$3[3+3D \;\; 6+6D] = (1+D)[9 \;\; 0] + (2+2D)[0 \;\; 9]$$

$$3[9 \;\; 0] = 3[0 \;\; 9] = [0 \;\; 0]$$

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

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-dim$(M) = 5$.

A particular 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?

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

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

are p-linearly independent.

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

A reduced p-basis for a submodule M of $\mathbb{Z}_{p^r}^n[D]$ gives rise to several invariants of M.

Let $V = (v_1(D), \ldots, v_k(D))$ be a reduced p-basis of M.

- The degrees of $v_1(D), \ldots, v_k(D)$ are called the **p-indices** of M;
- The **p-degree** of M is defined as the sum of the p-indices of M.

V.V. Vazirani, H. Saran and B.J. Rajan (1996)
An efficient algorithm for constructing minimal trellises for codes over finite abelian groups.
IEEE Trans. Information Theory, Vol. 42, pp. 1832-1854, 1996.

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.

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

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

A **reduced p-encoder** is a a polynomial matrix whose rows are a reduced p-basis of $\mathcal{C}$.
Note that all convolutional codes have a reduced p-encoder since every submodule of $\mathbb{Z}_{p^r}^n[D]$ has a reduced p-basis.

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

Block Codes

If a convolutional code admits a constant generator matrix, it is called a **block code**.

We introduce the notion of p-standard form from the definition of standard form.

Definition [G. H. Norton and A. Salagean, (2001)]

Let $\mathcal{C}$ be a block code over $\mathbb{Z}_{p^r}^n$. A generator matrix $\widetilde{G}$ for $\mathcal{C}$ is said to be in **standard form** if

$$\widetilde{G} = \begin{bmatrix} I_{k_0} & A_{1,0}^0 & A_{2,0}^0 & A_{3,0}^0 & \cdots & A_{r-1,0}^0 & A_{r,0}^0 \\ 0 & pI_{k_1} & pA_{2,1}^1 & pA_{3,1}^1 & \cdots & pA_{r-1,1}^1 & pA_{r,1}^1 \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{3,2}^2 & \cdots & p^2 A_{r-1,2}^2 & p^2 A_{r,2}^2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r,r-1}^{r-1} \end{bmatrix},$$

where the columns are grouped into blocks of sizes $k_0, \ldots, k_{r-1}, n - \sum_{i=0}^{r-1} k_i$.

[6] Graham H. Norton and Ana Salagean (2001)
On the Hamming distance of linear codes over a finite chain ring
IEEE Trans. Information Theory, Vol. 46-3, pp. 1060-1067, 2001.

Block Codes

Definition

Let $\mathcal{C}$ be a block code over $\mathbb{Z}_{p^r}^n[D]$. A p-encoder G of $\mathcal{C}$ is said to be in **p-standard form** if

$$G = \left[\begin{array}{ccccccc}
I_{k_0} & A_{1,0}^0 & A_{2,0}^0 & A_{3,0}^0 & \cdots & A_{r-1,0}^0 & A_{r,0}^0 \\
\hline
pI_{k_0} & 0 & pA_{2,1}^0 & pA_{3,1}^0 & \cdots & pA_{r-1,1}^0 & pA_{r,1}^0 \\
0 & pI_{k_1} & pA_{2,1}^1 & pA_{3,1}^1 & \cdots & pA_{r-1,1}^1 & pA_{r,1}^1 \\
\hline
p^2 I_{k_0} & 0 & 0 & p^2 A_{3,2}^0 & \cdots & p^2 A_{r-1,2}^0 & p^2 A_{r,2}^0 \\
0 & p^2 I_{k_1} & 0 & p^2 A_{3,2}^1 & \cdots & p^2 A_{r-1,2}^1 & p^2 A_{r,2}^1 \\
0 & 0 & p^2 I_{k_2} & p^2 A_{3,2}^2 & \cdots & p^2 A_{r-1,2}^2 & p^2 A_{r,2}^2 \\
\hline
\vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\
\hline
p^{r-1} I_{k_0} & 0 & 0 & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^0 \\
0 & p^{r-1} I_{k_1} & 0 & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^1 \\
0 & 0 & p^{r-1} I_{k_2} & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^2 \\
0 & 0 & 0 & p^{r-1} I_{k_3} & \cdots & 0 & p^{r-1} A_{r,r-1}^3 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r,r-1}^{r-1}
\end{array}\right].$$

Definition

$G(D)$ is noncatastrophic if

$$v(D) = u(D)G(D) \text{ with finite support} \to u(D) \text{ finite support}$$

Definition

$G(D)$ is noncatastrophic if

$$v(D) = u(D)G(D) \text{ with finite support } \to u(D) \text{ finite support}$$

Open problem

any convolutional code over $\mathbb{Z}_{p^r}^n[D]$ admits a noncatastrophic p-encoder.

Conjecture

It was conjecture to be true.

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.

Free Distance

Main problem

How do we construct convolutional codes of a given length n, p-dimension k and p-degree δ with the largest possible distance?

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

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

$$\begin{aligned} k_0 + k_1 + \cdots + k_{r-1} &= \min_{k = rk'_0 + (r-1)k'_1 + \cdots + k'_{r-1}} (k'_0 + k'_1 + \cdots + k'_{r-1}) \\ &= \left\lceil \frac{k}{r} \right\rceil . \end{aligned}$$

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

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

$$\widetilde{k} = k_0 + k_1 + \cdots + k_{r-1},$$

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

[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, $i = 0, 1, \ldots, r-1,$.

The distance of $\widetilde{\mathcal{C}}$ equals (from [2])

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

From $\widetilde{k} = \lceil \frac{k}{r} \rceil$ 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 $G(D)$:

$$G(D) = \begin{bmatrix} \widetilde{G}_{k_0}(D) \\ p\widetilde{G}_{k_0}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_0}(D) \\ -\,-\,-- \\ p\widetilde{G}_{k_1}(D) \\ p^2\widetilde{G}_{k_1}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_1}(D) \\ -\,-\,-- \\ \vdots \\ -\,-\,-- \\ p^{r-1}\widetilde{G}_{k_{r-1}}(D) \end{bmatrix}.$$

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

- These constructions of MDS convolutional codes over $\mathbb{Z}_{p^r}$ are "based" on MDS convolutional codes over $\mathbb{Z}_p$.
- Lifting techniques: Solé et. al used the Hensel lifting of a cyclic code. We used direct lifting.
- The known constructions of a (n, k, δ)- convolutional code require very large fields.

Open problems

- What happens if we consider other metrics? Homogeneous weights?
- More general class of finite rings?
- Characterization and existence of the dual codes of a convolutional code over $\mathbb{Z}_{p^r}$

Thank you for your attention!

Thanks to the organizers!