2D convolutional codes

Raquel Pinto
University of Aveiro

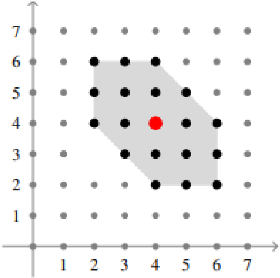
Workshop on Convolutional Codes, Zurich, 5-9 June

Overview

- 2D convolutional codes (Fornasini,Valcher,94; Weiner,Rosenthal,94)
- MDS 2D convolutional codes
- Decoding of 2D convolutional codes

2D (two-dimensional) data

- representation of pictures or videos;
- storage of digital data information.



$$\{u(4,2), u(5,2), u(6,2), u(3,3), u(4,3), u(5,3), u(6,3), u(2,4),$$
$$u(3,4), u(4,4), u(5,4), u(6,4), u(2,5), u(3,5), u(4,5), u(5,5), u(2,6),$$
$$u(3,6), u(4,6)\}, \quad u(i,j) \in \mathbb{F}^k$$

$$\{u(i,j) : u(i,j) \in \mathbb{F}^k, (i,j) \in \mathbb{N}^2\} \text{ with finite support}$$

$$\downarrow$$

$$u(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} u(i,j) z_1^i z_2^j \in \mathbb{F}^k[z_1, z_2] \simeq \mathbb{F}[z_1, z_2]^k$$

Former example:

$$u(z_1, z_2) = u(4,2) z_1^4 z_2^2 + u(5,2) z_1^5 z_2^2 + \cdots + u(4,6) z_1^4 z_2^6$$

2D convolutional codes

Definition

A two-dimensional (2D) (n, k) convolutional code $\mathcal{C}$ is a free $\mathbb{F}[z_1, z_2]$-submodule of $\mathbb{F}[z_1, z_2]^n$ of rank k.

A matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ whose rows form a basis for $\mathcal{C}$ is called an encoder.

$$\begin{aligned} \mathcal{C} &= \mathrm{Im}_{\mathbb{F}[z_1, z_2]} G(z_1, z_2) \\ &= \left\{ v(z_1, z_2) = u(z_1, z_2) G(z_1, z_2) :\ u(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k \right\} \end{aligned}$$

Definition

$U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times k}$ is unimodular if it has a polynomial inverse.

Lemma

$U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times k}$ is unimodular iff det $U(z_1, z_2) \in \mathbb{F}\backslash\{0\}$.

Definition

$G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$, with $n \geq k$, is,

1. left factor prime (ℓFP) if for every factorization

$$G(z_1, z_2) = T(z_1, z_2)\bar{G}(z_1, z_2),$$

   with $\bar{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$ and $T(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times k}$, then $T(z_1, z_2)$ is unimodular.
2. left zero prime (ℓZP) if the ideal generated by the $k \times k$ minors of $G(z_1, z_2)$ is $\mathbb{F}[z_1, z_2]$.

Lemma

Let $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ *be an encoder of* $\mathcal{C}$*. Then* $\bar{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ *is an encoder of* $\mathcal{C}$ *if and only if*

$$\bar{G}(z_1, z_2) = U(z_1, z_2) G(z_1, z_2),$$

for some unimodular matrix $U(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times k}$*.*

Thus:

- if $\mathcal{C}$ admits a left factor prime encoder, all its encoders are left factor prime encoders;
- if $\mathcal{C}$ admits a left zero prime encoder, all its encoders are left zero prime encoders.

Lemma

Let $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$. *Then*

1. $G(z_1, z_2)$ *is* ℓFP *if and only if for all* $u(z_1, z_2) \in \mathbb{F}(z_1, z_2)^k$, $u(z_1, z_2)G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^n \Rightarrow u(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k$.
2. $G(z_1, z_2)$ *is* ℓZP *if and only if* $G(z_1, z_2)$ *admits a polynomial right inverse.*

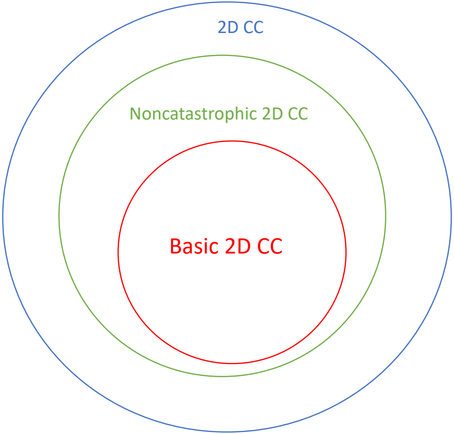
- A 2D convolutional code that admits a left factor prime encoder is said to be noncatastrophic.
- A 2D convolutional code that admits a left zero prime encoder is said to be basic.

Example

The 2D convolutional code with encoder

$$G(z_1, z_2) = \left[\begin{array}{cc} z_1 & z_2 \end{array}\right]$$

is noncatastrophic but it is not basic.



Lemma

A 2D (n, k)convolutional code is noncatastrophic if and only if there exists a full row rank matrix $H(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{(n-k)\times n}$ such that

$$\mathcal{C} = \{v(z_1, z_2) \in \mathbb{F}[z_1, z_2]^n \,:\, H(z_1, z_2)v(z_1, z_2)^T = 0\}.$$

MDS 2D convolutional codes

The (total) degree of a polynomial $p(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} p_{ij} z_1^i z_2^j$ in two indeterminates is defined as

$$max\{i + j : p_{ij} \neq 0\}$$

The i-th row degree of a matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$ is the maximum of the degrees of the polynomials in this row, and we call the external degree of $G(z_1, z_2)$ as the sum of its row degrees.

The internal degree of a matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times n}$ is the maximum of the degrees of full size minors of $G(z_1, z_2)$.

Definition

The degree, δ, of $\mathcal{C}$ is the minimum of the external degrees of the encoders of $\mathcal{C}$ and $\mathcal{C}$ is said to be an (n, k, δ) convolutional code.

Definition

The complexity, δ_c, of $\mathcal{C}$ is the internal degree of an encoder.

Obviously, $\delta_c \leq \delta$.

Example

The 2D convolutional code with encoder

$$G(z_1, z_2) = \begin{bmatrix} 0 & z_2 & 1 \\ 1 & z_1 & 1 \end{bmatrix}$$

has complexity $\delta_c = 1$ and degree $\delta = 2$.

Distance

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

$$d(\mathcal{C}) = \{wt(v(z_1, z_2)) : v(z_1, z_2) \in \mathcal{C}, v(z_1, z_2) \neq 0\}$$

where $wt(v(z_1, z_2))$ is the weight of a polynomial vector

$$v(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}^2} v_{ij} z_1^i z_2^j \in \mathbb{F}^n[z_1, z_2]$$

given by

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

Theorem (Climent,Napp,Perea,P.,2015)

Let $\mathcal{C}$ be a 2D (n, k, δ) convolutional code. Then

$$d(\mathcal{C}) \leq n\frac{(\lfloor\frac{\delta}{k}\rfloor + 1)(\lfloor\frac{\delta}{k}\rfloor + 2)}{2} - k(\lfloor\frac{\delta}{k}\rfloor + 1) + \delta + 1$$

This upper bound is called the 2D generalized Singleton bound.

A 2D (n, k, δ) convolutional code is said to be a Maximum Distance Separable (MDS) 2D convolutional code if its distance equals the generalized Singleton bound.

Constructions of 2D MDS convolutional codes

Lemma

If $\mathcal{C}$ is a MDS (n, k, δ) 2D convolutional code then $\mathcal{C}$ has an encoder $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ with $t = k - \delta + k\lfloor \frac{\delta}{k} \rfloor$ rows of degree $\lfloor \frac{\delta}{k} \rfloor$ and $k - t$ rows of degree $\lfloor \frac{\delta}{k} \rfloor + 1$.

Note that a row with degree $\lfloor \frac{\delta}{k} \rfloor$ has $\ell_1 = \frac{(\lfloor \frac{\delta}{k} \rfloor + 1)(\lfloor \frac{\delta}{k} \rfloor + 2)}{2}$ coefficients in $\mathbb{F}^n$ and a row with degree $\lfloor \frac{\delta}{k} \rfloor + 1$ has $\ell_2 = \frac{(\lfloor \frac{\delta}{k} \rfloor + 2)(\lfloor \frac{\delta}{k} \rfloor + 3)}{2}$ coefficients in $\mathbb{F}^n$.

Let us construct an encoder $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ with the first $k - t$ rows of degree $\lfloor \frac{\delta}{k} \rfloor + 1$ and the last t rows of degree $\lfloor \frac{\delta}{k} \rfloor$ (Climent,Napp,Perea, P.,2016).

Consider the matrices,

$$\mathcal{G}_r = \begin{cases} \begin{bmatrix} g_0^{(r)} \\ g_1^{(r)} \\ \vdots \\ g_{\ell_2-1}^{(r)} \end{bmatrix} \in \mathbb{F}^{\ell_2 \times n} \text{ for } r = 1, 2, \ldots, k-t. \\ \\ \begin{bmatrix} g_0^{(r)} \\ g_1^{(r)} \\ \vdots \\ g_{\ell_1-1}^{(r)} \end{bmatrix} \in \mathbb{F}^{\ell_1 \times n} \text{ for } r = k-t+1, k-t+2, \ldots, k. \end{cases}$$

$$G(z_1, z_2) = \begin{bmatrix} G_1(z_1, z_2) \\ G_2(z_1, z_2) \\ \vdots \\ G_k(z_1, z_2) \end{bmatrix} \in \mathbb{F}[z_1, z_2]^{n \times k}$$

with

$$G_r(z_1, z_2) = \begin{cases} \displaystyle\sum_{0 \le i+j \le \lfloor \frac{\delta}{k} \rfloor + 1} g^{(r)}_{\mu(i,j)} z_1^i z_2^j & \text{for } r = 1, 2, \ldots, k-t \\ \displaystyle\sum_{0 \le i+j \le \lfloor \frac{\delta}{k} \rfloor} g^{(r)}_{\mu(i,j)} z_1^i z_2^j & \text{for } r = k-t+1, \ldots, k \end{cases}$$

where $\mu(i,j) = j + \frac{(i+j)(i+j+1)}{2}$.

Consider also

$$\bar{\mathcal{G}}_r = \begin{cases} \begin{bmatrix} g_0^{(r)} & g_1^{(r)} & \cdots & g_{\ell_2-1}^{(r)} \end{bmatrix} \text{ for } r = 1, 2, \ldots, k-t. \\ \\ \begin{bmatrix} g_0^{(r)} & g_1^{(r)} & \cdots & g_{\ell_1-1}^{(r)} \end{bmatrix} \text{ for } r = k-t+1, k-t+2, \ldots, k. \end{cases}$$

If

$$\mathcal{G} = \begin{bmatrix} \mathcal{G}_1 \\ \mathcal{G}_2 \\ \vdots \\ \mathcal{G}_k \end{bmatrix}$$

is full superregular and

$$\bar{\mathcal{G}} = \begin{bmatrix} \bar{\mathcal{G}}_1 & \\ \vdots & \\ \bar{\mathcal{G}}_{k-t} & \\ \bar{\mathcal{G}}_{k-t+1} & 0 \\ \vdots & \\ \bar{\mathcal{G}}_k & 0 \end{bmatrix}$$

is superregular, then $G(z_1, z_2)$ is an encoder of an MDS (n, k, δ) 2D convolutional code if $n \geq \ell_2 k$.

- Constructions of MDS (n, k, δ) 2D convolutional codes if $n > k + \delta$ (Almeida, Napp, P., 2018).

Decoding of 2D convolutional codes

There is no decoding algorithm over the q-ary symetric channel where errors occur.

Decoding algorithms over the erasure channel:
• using parity-check matrices (Climent, Napp, P., Simões, 2016).

Decoding algorithm over the erasure channel

(Lieb, P., 2023)

Let $\mathcal{C}$ be a 2D convolutional code and $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k \times n}$ be an encoder of $\mathcal{C}$.

Write

$$G(z_1, z_2) = G_0(z_1) + G_1(z_1)z_2 + G_2(z_1)z_2^2 + \cdots$$

and

$$u(z_1, z_2) = u_0(z_1) + u_1(z_1)z_2 + u_2(z_1)z_2^2 + \cdots \in \mathbb{F}^k[z_1, z_2]$$

Then

$$
\begin{aligned}
v(z_1, z_2) &= u(z_1, z_2)G(z_1, z_2) \\
&= u_0(z_1)G_0(z_1) + (u_1(z_1)G_0(z_1) + u_0(z_1)G_1(z_1))z_2 + \\
&\quad +(u_2(z_1)G_0(z_1) + u_1(z_1)G_1(z_1) + u_0(z_1)G_2(z_1))z_2^2 + \cdots \\
&= u_0(z_1)G_0(z_1) + \begin{bmatrix} u_1(z_1) & u_0(z_1) \end{bmatrix} \begin{bmatrix} G_0(z_1) \\ G_1(z_1) \end{bmatrix} z_2 + \\
&\quad + \begin{bmatrix} u_2(z_1) & u_1(z_1) & u_0(z_1) \end{bmatrix} \begin{bmatrix} G_0(z_1) \\ G_1(z_1) \\ G_2(z_1) \end{bmatrix} z_2^2 \\
&\quad + \cdots
\end{aligned}
$$

Let ℓ be as large as possible such that

$$\mathcal{C}_0 = Im_{\mathbb{F}[z_1]} G_0(z_1), \quad \mathcal{C}_1 = Im_{\mathbb{F}[z_1]} \begin{bmatrix} G_0(z_1) \\ G_1(z_1) \end{bmatrix}, \cdots .$$

$$\mathcal{C}_\ell = Im_{\mathbb{F}[z_1]} \begin{bmatrix} G_0(z_1) \\ G_1(z_1) \\ \vdots \\ G_\ell(z) \end{bmatrix}$$

are full row rank (note that $k(\ell + 1) < n$).

Decoding (over the erasure channel)

Input data: received word

$$\tilde{v}(z_1, z_2) = \tilde{v}_0(z_1) + \tilde{v}_1(z_1)z_2 + \tilde{v}_2(z_1)z_2^2 + \cdots$$

1) let $i = \ell$;

2) $\tilde{v}_i(z_1)$ is a codeword of $\mathcal{C}_i$ with erasures;

3) recover the most number of erasures of $\tilde{v}_i(z)$ as possible;

3.1) if the the erasures of $\tilde{v}_i(z)$ are completely recovered and $v(z_1)$ is the corrected codeword, then compute $u_0(z_1), u_1(z_1), \dots, u_i(z_1)$ such that

$$v(z_1) = \begin{bmatrix} u_i(z_1) & u_{i-1}(z_1) & \dots & u_0(z_1) \end{bmatrix} \begin{bmatrix} G_0(z_1) \\ G_1(z_1) \\ \vdots \\ G_i(z_1) \end{bmatrix};$$

for $j \geq i$, let $\bar{v}_{i+j}(z_1) =$

$$\tilde{v}_{i+j}(z_1) - \begin{bmatrix} u_i(z_1) & u_{i-1}(z_1) & \cdots & u_0(z_1) \end{bmatrix} \begin{bmatrix} G_j(z_1) \\ \vdots \\ G_{i+j}(z_1) \end{bmatrix}$$ and

restart the decoding algorithm with input data

$$v(z_1, z_2) = \bar{v}_i(z_1) + \tilde{v}_{i+1}(z_1) z_2 + \tilde{v}_{i+2}(z_1) z_2^2 + \cdots$$

3.2) if the erasures of $\tilde{v}_i(z)$ are not completely recovered let $i := i - 1$ and go to 2)

Future work

- New constructions of MDS 2D convolutional codes.
- Decoding algorithms for error correction.
- Decoding algorithms for erasure correction - define an equivalent notion of column distances.

Thank you for your attention!

This work was supported by Fundação para a Ciência e a Tecnologia (FCT), within project UIBD/MAT/04106/2020 (CIDMA).