Center for Research and Development in Mathematics and Applications (CIDMA)
Department of Mathematics, University of Aveiro

Construction of an optimal convolutional code of rate 1/2

Zita Abreu
zita.abreu@ua.pt

July 11, 2022

Contents

Introduction

Introduction

- All real channels are noisy

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.
- Codes with longer distance are better

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.
- Codes with longer distance are better
- Free distance and the column distances

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.
- Codes with longer distance are better
- Free distance and the column distances
- Maximum Distance Separable (MDS) codes

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.
- Codes with longer distance are better
- Free distance and the column distances
- Maximum Distance Separable (MDS) codes
- Maximum Distance Profile (MDP) codes

Introduction

- All real channels are noisy $\longrightarrow$ Coding theory $\longrightarrow$ Convolutional Codes
- A **Convolutional Code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.
- Codes with longer distance are better
- Free distance and the column distances
- Maximum Distance Separable (MDS) codes
- Maximum Distance Profile (MDP) codes
- **PROBLEM:** Build convolutional codes with optimal distances

Main goal

Our main goal with this research was:

1. propose a new construction of convolutional codes. In particular, build convolutional codes with maximum free distance

Main concepts

Main concepts

A **convolutional code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.

Main concepts

A **convolutional code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.

A $k \times n$ matrix $G(D)$ with entries in $\mathbb{F}_q[D]$ whose rows constitute a basis of $\mathcal{C}$ is called a **generator matrix for** $\mathcal{C}$. This matrix is a full row rank matrix such that:

Main concepts

A **convolutional code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.

A $k \times n$ matrix $G(D)$ with entries in $\mathbb{F}_q[D]$ whose rows constitute a basis of $\mathcal{C}$ is called a **generator matrix for** $\mathcal{C}$. This matrix is a full row rank matrix such that:

$$\begin{aligned} \mathcal{C} &= \operatorname{Im}_{\mathbb{F}_q[D]} G(D) \\ &= \{v(D) \in \mathbb{F}_q[D]^n : v(D) = u(D)G(D) \text{ with } u(D) \in \mathbb{F}_q[D]^k\}. \end{aligned}$$

Main concepts

A **convolutional code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]-$ submodule of $\mathbb{F}_q[D]^n$ of rank k, where $\mathbb{F}_q[D]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$.

A $k \times n$ matrix $G(D)$ with entries in $\mathbb{F}_q[D]$ whose rows constitute a basis of $\mathcal{C}$ is called a **generator matrix for** $\mathcal{C}$. This matrix is a full row rank matrix such that:

$$\begin{aligned} \mathcal{C} &= \operatorname{Im}_{\mathbb{F}_q[D]} G(D) \\ &= \{v(D) \in \mathbb{F}_q[D]^n : v(D) = u(D)G(D) \text{ with } u(D) \in \mathbb{F}_q[D]^k\}. \end{aligned}$$

Two generator matrices $G_1(D),\ G_2(D) \in \mathbb{F}_q[D]^{k\times n}$ are said to be **equivalent generator matrices** if

$$\operatorname{Im}_{\mathbb{F}_q[D]} G_1(D) = \operatorname{Im}_{\mathbb{F}_q[D]} G_2(D),$$

which happens if and only if $G_1(D) = U(D)G_2(D)$ for some unimodular matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$.

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$
- For $i = 1, \cdots, n$: $\nu_i \equiv$ largest degree of any entry in row i of $G(D)$

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$
- For $i = 1, \cdots, n$: $\nu_i \equiv$ largest degree of any entry in row i of $G(D)$
- $\delta \leq \nu_1 + \nu_2 + \cdots + \nu_k$

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$
- For $i = 1, \cdots, n$: $\nu_i \equiv$ largest degree of any entry in row i of $G(D)$
- $\delta \leq \nu_1 + \nu_2 + \cdots + \nu_k$
- External degree $\equiv \sum_{i=1}^{k} \nu_i$

Let $G(D) \in \mathbb{F}_q[D]^{k \times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$
- For $i = 1, \cdots, n$: $\nu_i \equiv$ largest degree of any entry in row i of $G(D)$
- $\delta \leq \nu_1 + \nu_2 + \cdots + \nu_k$
- External degree $\equiv \sum_{i=1}^{k} \nu_i$
- Internal degree = External degree $\longrightarrow$ $G(D)$ is said to be row reduced and it is called a **minimal generator matrix**

Let $G(D) \in \mathbb{F}_q[D]^{k\times n}$ be a generator matrix.

- Internal degree (δ) $\equiv$ maximal degree of the full size minors of $G(D)$
- For $i = 1, \cdots, n$: $\nu_i \equiv$ largest degree of any entry in row i of $G(D)$
- $\delta \leq \nu_1 + \nu_2 + \cdots + \nu_k$
- External degree $\equiv \sum_{i=1}^{k} \nu_i$
- Internal degree = External degree $\longrightarrow$ $G(D)$ is said to be row reduced and it is called a **minimal generator matrix**
- The **degree** of a code is the external degree of a minimal generator matrix.

The **free distance** of a convolutional code is defined as:

$$d_{free}(\mathcal{C}) = \min\{wt(v(D))|v(D) \in \mathcal{C}, v(D) \neq 0\},$$

where $wt(v(D))$ is the Hamming weight of a polynomial vector $v(D) = \sum_{t=0}^{\deg(v(D))} v_t D^t \in \mathbb{F}_q[D]^n$ that is defined as

$$wt(v(D)) = \sum_{t=0}^{\deg(v(D))} wt(v_t),$$

where the weight $wt(v)$ of $v \in \mathbb{F}_q^n$ is the number of nonzero components of v.

The **free distance** of a convolutional code is defined as:

$$d_{free}(\mathcal{C}) = \min\{wt(v(D))|v(D) \in \mathcal{C}, v(D) \neq 0\},$$

where $wt(v(D))$ is the Hamming weight of a polynomial vector $v(D) = \sum_{t=0}^{\deg(v(D))} v_t D^t \in \mathbb{F}_q[D]^n$ that is defined as

$$wt(v(D)) = \sum_{t=0}^{\deg(v(D))} wt(v_t),$$

where the weight $wt(v)$ of $v \in \mathbb{F}_q^n$ is the number of nonzero components of v.

Maximum distance separable (MDS) codes have maximum free distance in the class of convolutional codes of rate k/n and degree δ , i.e., are the ones with free distance equal to the generalized **Singleton bound** (upper bound)

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

Main idea

Main idea

Consider a generator matrix $G(D)$ of a convolutional code over a field $\mathbb{F}_q$ and construct a generator matrix of a new convolutional code over the same field $\mathbb{F}_q$ and of higher degree, by repeating the coefficients of $G(D)$ of certain degrees.

Advantage

- Build a convolutional code MDS defined over a smaller field than the existing constructions of MDS convolutional codes with the same degree.

Justesen's Theorem

Theorem ([4])

For $n \geq 2$ and $|\mathbb{F}_q| \geq n+1$, set $s_j := \lceil (j-1)(|\mathbb{F}_q|-1)/n \rceil$ for $j = 2, \cdots, n$ and

$$\delta := \begin{cases} \left\lfloor \frac{2}{9}|\mathbb{F}_q| \right\rfloor & \text{if } n = 2, \\ \left\lfloor \frac{1}{3}|\mathbb{F}_q| \right\rfloor & \text{if } 3 \leq n \leq 5, \\ \left\lfloor \frac{1}{2}|\mathbb{F}_q| \right\rfloor & \text{if } n \geq 6 \end{cases}$$

Moreover, let α be a primitive element of $\mathbb{F}_q$, and set

$$g_1(x) := \prod_{k=1}^{\delta} (x - \alpha^k),$$

$$g_j(x) := g_1(x\alpha^{-s_j})$$

for $j = 2, \cdots, n$. Then

$$G(D) = [g_1(D) \cdots g_n(D)]$$

is the generator matrix of an MDS $(n, 1, \delta)$ convolutional code with free distance equal to $n(\delta+1)$.

New construction

Let $n = 2$ and $\delta = 2$

New construction

Let $n = 2$ and $\delta = 2 \longrightarrow \mathbb{F}_{11}, \mathbb{F}_{13}$

New construction

Let $n = 2$ and $\delta = 2 \longrightarrow \mathbb{F}_{11}, \mathbb{F}_{13}$

Construction Idea

Let α be a primitive element of $\mathbb{F}_q$, with $q = 11, 13$. Then

$$\tilde{G}(D) = G_0 + G_1 D + G_2 D^2 + G_2 D^3 + G_1 D^4 + G_0 D^5, \text{ with}$$

$$G_0 = \begin{bmatrix} \alpha^3 & \alpha^3 \end{bmatrix}$$

$$G_1 = \begin{bmatrix} -\alpha^2 - \alpha & \alpha^{-s_j}(-\alpha^2 - \alpha) \end{bmatrix}$$

$$G_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

is the generator matrix of a $(2, 1, 5)$ MDS convolutional code.

Primitive elements (α):

- $\mathbb{F}_{11}$: $2, 6, 7, 8$
- $\mathbb{F}_{13}$: $2, 6, 7, 11$

Primitive elements (α):

- $\mathbb{F}_{11}$: $2, 6, 7, 8$
- $\mathbb{F}_{13}$: $2, 6, 7, 11$

Theorem (Construction)

Let $\alpha = 2$ be a primitive element of $\mathbb{F}_{11}$. Then

$$\tilde{G}(D) = G_0 + G_1 D + G_2 D^2 + G_2 D^3 + G_1 D^4 + G_0 D^5,$$

with $G_0 = \begin{bmatrix} 8 & 8 \end{bmatrix}$, $G_1 = \begin{bmatrix} 5 & 6 \end{bmatrix}$ and $G_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$ is the generator matrix of a $(2, 1, 5)$ MDS convolutional code.

Theorem (Construction)

Let $\alpha = 6$ be a primitive element of $\mathbb{F}_{11}$. Then

$$\tilde{G}(D) = G_0 + G_1 D + G_2 D^2 + G_2 D^3 + G_1 D^4 + G_0 D^5,$$

with $G_0 = \begin{bmatrix} 7 & 7 \end{bmatrix}$, $G_1 = \begin{bmatrix} 2 & 9 \end{bmatrix}$ and $G_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$ is the generator matrix of a $(2, 1, 5)$ MDS convolutional code.

Construction Idea

$$\mathbb{F}_q \text{ with } q \text{ prime}$$
$$\downarrow$$
$$\mathbb{F}_{p^k} \text{ with } p \text{ prime}$$
$$\downarrow$$
$$\mathbb{F}_9$$

Construction Idea

$$\mathbb{F}_q \text{ with } q \text{ prime}$$
$$\downarrow$$
$$\mathbb{F}_{p^k} \text{ with } p \text{ prime}$$
$$\downarrow$$
$$\mathbb{F}_9$$

$\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$

- Primitive elements: $\alpha + 1, \alpha + 2, 2\alpha + 1, 2\alpha + 2$

Future work

Parameters

- δ
- n

References


R. Johannesson, K.S. Zigangirov, Fundamentals of Convolutional Coding, Digital and Mobile Communication, Wiley-IEEE Press, New Jersey, 1999.


Lieb, J.; Pinto, R.; Rosenthal, J.: Convolutional Codes, in "Concise Encyclopedia of Coding Theory" (eds. Huffman, C; Kim, J.; Sole, P.), CRC Press, 2021.


R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal, Constructions for MDS-convolutional codes, IEEE Trans. Inform. Theory, 47(5), pp. 2045-2049, 2001.


J. Rosenthal and R. Smarandache, Maximum distance separable convolutional codes, Appl. Algebra Engrg. Comm. Comput, 10.1, pp. 15-32, 1999.


J. Justesen, An algebraic construction of rate $1/\nu$ convolutional codes, IEEE Trans. Inform. Theory, 21.1, pp. 577-580, 1975.


R. Smarandache and J. Rosenthal, A State Space Approach for Constructing MDS Rate $1/n$ Convolutional Codes, Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory, pp. 116-117., 1998.


H. Gluesing-Luerssen and B. Langfeld, A Class of one-dimensional MDS convolutional codes, Journal of Algebra and Its Applications, 5.4, pp. 505-520, 2006.

Thank you for your attention

Acknowledgments

This work was supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), UIDB/04106/2020 and UIDP/04106/2020. Zita Abreu is also supported by FCT grant UI/BD/151186/2021.