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 3, 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 1:

- Basics,
- From block codes to convolutional codes
- Encoders

Basic Problem:

- want to store bits on magnetic storage device
- or send a message (sequence of zeros/ones)

Day 1:

- Basics,
- From block codes to convolutional codes
- Encoders

Basic Problem:

- want to store bits on magnetic storage device
- or send a message (sequence of zeros/ones)
- Bits get corrupted, $0 \to 1$ or $1 \to 0$, but rarely.

Day 1:

- Basics,
- From block codes to convolutional codes
- Encoders

Basic Problem:

- want to store bits on magnetic storage device
- or send a message (sequence of zeros/ones)

- Bits get corrupted, $0 \to 1$ or $1 \to 0$, but rarely.

What happens when we store/send information and errors occur?

Day 1:

- Basics,
- From block codes to convolutional codes
- Encoders

Basic Problem:

- want to store bits on magnetic storage device
- or send a message (sequence of zeros/ones)
- Bits get corrupted, $0 \to 1$ or $1 \to 0$, but rarely.

What happens when we store/send information and errors occur?

can we detect them? correct?

The International Standard Book Number (ISBN)

It can be proved that all possible valid ISBN-10's have at least two digits different from each other.
ISBN-10:

$$x_1 - x_2x_3x_4 - x_5x_6x_7x_8x_9 - x_{10}$$

satisfy

$$\sum_{i=1}^{10} ix_i = 0 \quad mod \quad 11$$

For example, for an ISBN-10 of 0-306-40615-2:

$$\begin{aligned} s &= (0 \times 10) + (3 \times 9) + (0 \times 8) + (6 \times 7) + \\ &+ (4 \times 6) + (0 \times 5) + (6 \times 4) + (1 \times 3) + (5 \times 2) + (2 \times 1) \\ &= 0 + 27 + 0 + 42 + 24 + 0 + 24 + 3 + 10 + 2 \\ &= 132 = 12 \times 11 \end{aligned}$$

- Break the message into 3 bits blocks $m = \boxed{1}\boxed{1}\boxed{0} \in \mathbb{F}^3$
- Encode each block as follows:

$$u \longrightarrow uG \qquad G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix};$$

- Break the message into 3 bits blocks $m = \boxed{1 \mid 1 \mid 0} \in \mathbb{F}^3$
- Encode each block as follows:

$$u \longrightarrow uG \qquad G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix};$$

For example

$$(1,\ 1,\ 0) \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1,\ 1,\ 0,\ 0,\ 1,\ 1);$$

$$(1,\ 0,\ 1) \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1,\ 0,\ 1,\ 1,\ 0,\ 1);$$

etc...

- Only 2^3 codewords in $\mathbb{F}^6$

$$\mathcal{C} = \{(1,0,0,1,1,0),(0,1,0,1,0,1),(0,0,1,0,1,1),(1,1,0,0,1,1),$$

$$(1,0,1,1,0,1),(0,1,1,1,1,0),(1,1,1,0,0,0),(0,0,0,0,0,0)\}$$

- In $\mathbb{F}^6$ we have 2^6 possible vectors

- Only 2^3 codewords in $\mathbb{F}^6$

$$\mathcal{C} = \{(1,0,0,1,1,0),(0,1,0,1,0,1),(0,0,1,0,1,1),(1,1,0,0,1,1),$$

$$(1,0,1,1,0,1),(0,1,1,1,1,0),(1,1,1,0,0,0),(0,0,0,0,0,0)\}$$

- In $\mathbb{F}^6$ we have 2^6 possible vectors

- Any two codewords differ at least in 3 coordinates. I can detect and correct 1 error!!!

- Coding theory develops methods to protect information against errors.
- Cryptography develops methods how to protect information against an enemy (or an unauthorized user).
- Coding theory - theory of error correcting codes - is one of the most interesting and applied part of mathematics and informatics.
- All real systems that work with digitally represented data, as CD players, TV, fax machines, internet, satelites, mobiles, require to use error correcting codes because all real channels are, to some extent, noisy.
- Coding theory methods are often elegant applications of very basic concepts and methods of (abstract) algebra.

Let's start: Block codes

$$\begin{aligned} \Phi : \mathbb{F}^k &\rightarrow \mathbb{F}^n \\ u &\rightarrow \Phi(u) = v = uG \end{aligned}$$

u information word, v codeword and G the encoder.

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}} G = \left\{ uG : u \in \mathbb{F}^k \right\},$$

i.e., a k-dimensional vector subspace of $\mathbb{F}^n$ over $\mathbb{F}$.

If we have a sequence of information words

$$u(0), u(1), \cdots \longrightarrow v(0), v(1), \ldots$$

i.e.

$$u(i) \longrightarrow u(i)G = v(i).$$

Let me rewrite sequences as polynomials

$$\{u(0), u(1), \dots\} \Rightarrow u(0) + u(1)D + u(2)D^2 + \dots$$

and

$$\{v(0), v(1), \dots\} \Rightarrow v(0) + v(1)D + v(2)D^2 + \dots$$

Then

$$\sum_{i\geq 0} u(D) \longrightarrow \sum_{i\geq 0} u(D)G = \sum_{i\geq 0} v(D)$$

Laurent series of interest

- Power series: $\sum_{i\geq 0} s(D)$. It is an integral domain, $\mathbb{F}[[D]]$.
- Laurent series: $\sum_{i\geq m} s(D)$. It is a field, $\mathbb{F}((D))$.
- Polynomials: $\mathbb{F}[D]$. Power series with finite support.
- Rational functions: $P(D)/Q(D)$ ($Q(D) \neq 0$) has unique Laurent expansion as a Laurent series.
- Realizable Laurent series: $P(D)/Q(D)$ ($Q(0) \neq 0$).

Elias' idea 1955

Block codes

$$\sum_{i\geq 0} u(D) \longrightarrow \sum_{i\geq 0} u(D)G = \sum_{i\geq 0} v(D)$$

Why not G polynomial??

Elias' idea 1955

Block codes

$$\sum_{i\geq 0} u(D) \longrightarrow \sum_{i\geq 0} u(D)G = \sum_{i\geq 0} v(D)$$

Why not G polynomial??

Convolutional codes

$$\sum_{i\geq 0} u(D) \longrightarrow \sum_{i\geq 0} u(D)G(D) = \sum_{i\geq 0} v(D)$$

Block codes vs convolutional codes

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

Convolutional code

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

Block codes vs convolutional codes

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

Convolutional code

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

Definition

An (n, k) convolutional code is a k-dimensional subspace of $\mathbb{F}(D)^n$.

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

Remark

If consider only codewords with finite support, a convolutional code of rate k/n is a $\mathbb{F}[D]$-submodule of $\mathbb{F}^n[D]$ of rank k.

Example

Let $G(D) = \begin{pmatrix} 1+D+D^2 & 1+D^2 \end{pmatrix}$. This encoder has memory 2. Assume that we want to encode the string

$$1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ldots$$

which in polynomial form gives $u(D) = 1 + D^3 + D^4 + D^6 + D^7 + \dots$.

Example

Let $G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$. This encoder has memory 2. Assume that we want to encode the string

$$1\ 0\ 0\ 1\ 1\ 0\ 1\ 1 \ldots$$

which in polynomial form gives $u(D) = 1 + D^3 + D^4 + D^6 + D^7 + \ldots$. Doing the product $u(D)G(D)$, we obtain

$$\begin{aligned}(v_0(D), v_1(D)) = \quad & (1 + D + D^2 + D^3 + 0D^4 + 0D^5 + 0D^6 + \ldots, \\ & 1 + 0D + D^2 + D^3 + D^4 + D^5 + 0D^6 + D^7 + \ldots)\end{aligned}$$

Example

Let $G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$. This encoder has memory 2. Assume that we want to encode the string

$$1\ 0\ 0\ 1\ 1\ 0\ 1\ 1 \ldots$$

which in polynomial form gives $u(D) = 1 + D^3 + D^4 + D^6 + D^7 + \ldots$. Doing the product $u(D)G(D)$, we obtain

$$\begin{aligned}(v_0(D), v_1(D)) = \quad & (1 + D + D^2 + D^3 + 0D^4 + 0D^5 + 0D^6 + \ldots, \\ & 1 + 0D + D^2 + D^3 + D^4 + D^5 + 0D^6 + D^7 + \ldots)\end{aligned}$$

Interleaving the coefficients, we obtain that the encoding string is

$$11\ 10\ 11\ 11\ 01\ 01\ 00\ 01 \ldots$$

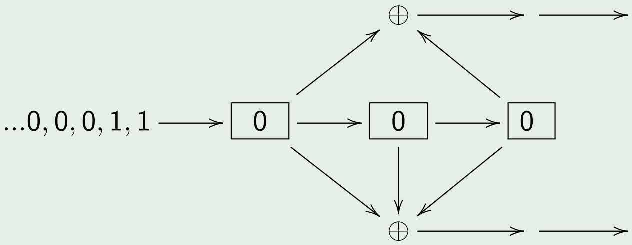
Viewed as computer scientists

Example

With Shift Registers:

$$G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$$

has the following implementation

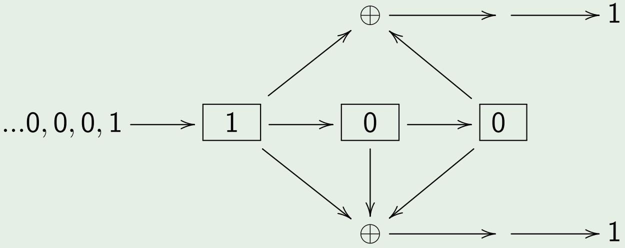


Example

The encoder

$$G(D) = \left(\begin{array}{cc} 1 + D + D^2 & 1 + D^2 \end{array} \right)$$

has the following implementation

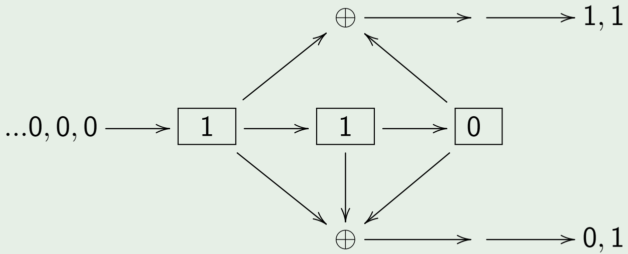


Example

The encoder

$$G(D) = \left(\begin{array}{cc} 1 + D + D^2 & 1 + D^2 \end{array} \right)$$

has the following implementation

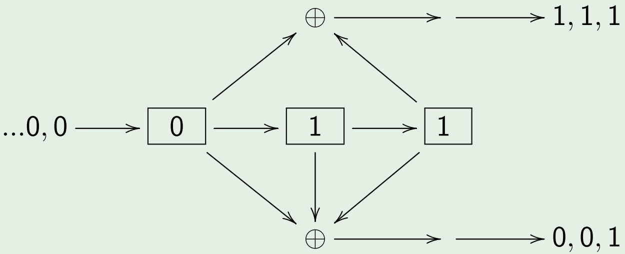


Example

The encoder

$$G(D) = \begin{pmatrix} 1+D+D^2 & 1+D^2 \end{pmatrix}$$

has the following implementation

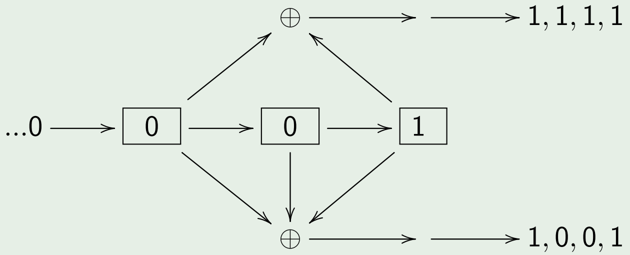


Example

The encoder

$$G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$$

has the following implementation

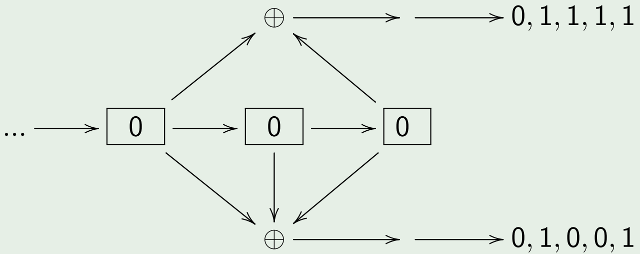


Example

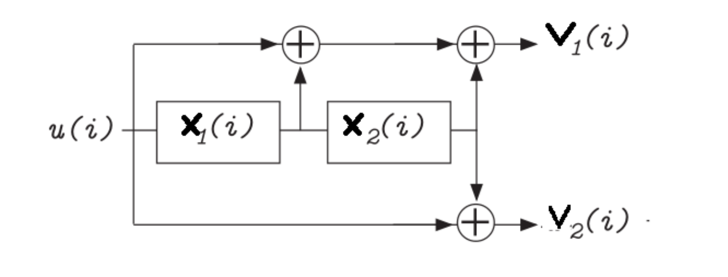
The encoder

$$G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$$

has the following implementation



Example



A physical realization for the encoder $G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}$.
This encoder has degree 2 and memory 2.

A convolutional encoder is *also* a linear device which maps

$$u(0), u(1), \cdots \longrightarrow v(0), v(1), \ldots$$

In this sense it is the <u>same</u> as block encoders. The <u>difference</u> is that the convolutional encoder has an internal "storage vector" or "memory".

A convolutional encoder is *also* a linear device which maps

$$u(0), u(1), \cdots \longrightarrow v(0), v(1), \ldots$$

In this sense it is the same as block encoders. The difference is that the convolutional encoder has an internal "storage vector" or "memory".

Definition

Remember: Convolutional code are k-dimensional subspace of $\mathbb{F}(D)^n$.

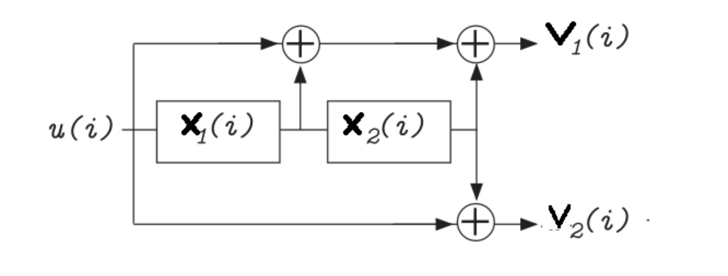
$$\mathcal{C} \;=\; \mathrm{Im}_{\mathbb{F}(D)} G(D) = \left\{ u(D)G(D) : \; u(D) \in \mathbb{F}^k(D) \right\}$$

Polynomial Generator Matrices

Two encoders $G(D), G'(D)$ are equivalent if they generate the same code, i.e., if they are $\mathbb{F}(D)$-row equivalent. In other words, there exist a nonsingular matrix $U(D)$ such that

$$G(D) = U(D)G'(D)$$

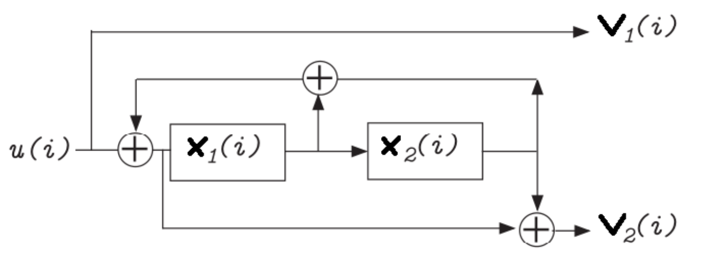
Example



A physical realization for the encoder $G(D) = \begin{pmatrix} 1+D+D^2 & 1+D^2 \end{pmatrix}$.
This encoder has degree 2 and memory 2.
Clearly any matrix which is $\mathbb{F}(D)$-equivalent to $G(D)$ is also an encoder.

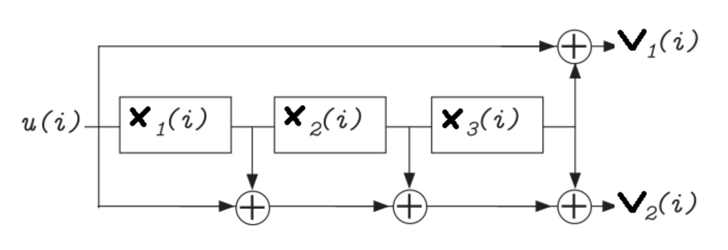
$$G'(D) = \begin{pmatrix} 1 & \frac{1+D^2}{1+D+D^2} \end{pmatrix}$$

Example



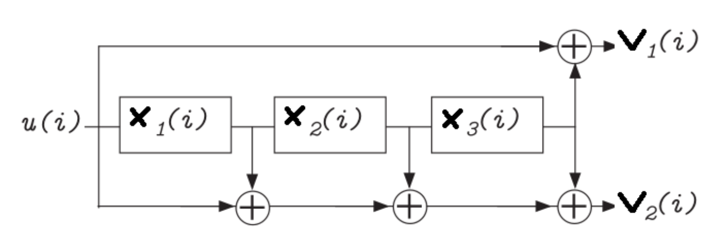
A physical realization for an equivalent encoder $G'(D)$. This encoder has degree 2 and infinite memory.

Example



A physical realization for the (catastrophic) equivalent encoder $G''(D) = (1 + D)G(D) = \begin{pmatrix} 1 + D^3 & 1 + D + D^2 + D^3 \end{pmatrix}$. This encoder has degree 3 and memory 3.

Example



A physical realization for the (catastrophic) equivalent encoder $G''(D) = (1+D)G(D) = \begin{pmatrix} 1+D^3 & 1+D+D^2+D^3 \end{pmatrix}$. This encoder has degree 3 and memory 3.

Then...

- .which encoders are *good*?
- which are *minimal*?
- are there *canonical* forms?

Properties of Encoders

Definition

If the entries of $G(D)$ are polynomials, $G(D)$ is called polynomial encoder (PE). PE are interesting because they have finite memory (no feedback loop in the implementation).

Properties of Encoders

Definition

If the entries of $G(D)$ are polynomials, $G(D)$ is called polynomial encoder (PE). PE are interesting because they have finite memory (no feedback loop in the implementation).

Definition

Let $G(D)$ be a PE.

1. Internal degree of $G(D)$ = maximum degree of $G(D)$'s $k \times k$ minors
2. External degree of $G(D)$= sum of the row degree of $G(D)$
3. $G(D)$ is basic if among all encoders has the minimum possible internal degree
4. $G(D)$ is reduced if among all encoders has the minimum possible external degree

Properties of Encoders

Definition

If the entries of $G(D)$ are polynomials, $G(D)$ is called polynomial encoder (PE). PE are interesting because they have finite memory (no feedback loop in the implementation).

Definition

Let $G(D)$ be a PE.

1. Internal degree of $G(D)$ = maximum degree of $G(D)$'s $k \times k$ minors
2. External degree of $G(D)$= sum of the row degree of $G(D)$
3. $G(D)$ is basic if among all encoders has the minimum possible internal degree
4. $G(D)$ is reduced if among all encoders has the minimum possible external degree

Note that Internal degree $G(D) \leq$ External degree $G(D)$

Theorem

Let $G(D) \in \mathbb{F}^{k \times n}$. The following are equivalent:

- $G(D)$ is basic
- The gcd of the $k \times k$ minors of $G(D)$ is 1
- $G(\alpha)$ has rank k for any α in the algebraic closure of $\mathbb{F}$.
- $G(D)$ has a *polynomial* right inverse, i.e., $\exists T(D)$ such that $G(D)T(D) = I_k$.
- There exists a parity-check matrix $H(D) \in \mathbb{F}[D]^{n-k \times n}$, i.e., a matrix such that $\mathcal{C} = \{v(D) \in \mathbb{F}(D)^n \mid H(D)v(D) = 0\}$.

Example

Is $G(D) = \begin{pmatrix} D^2+1 & D^3+1 \end{pmatrix}$ basic?
Not. $(D+1) \neq 1$ is the gcd of its 1×1 minors, equivalently $G(1) = 0$.
Multiply by $(D+1)^{-1}$ to obtain the equivalent basic encoder

$$\overline{G}(D) = \begin{pmatrix} D+1 & D^2+D+1 \end{pmatrix}$$

Theorem

The following are equivalent:

- $G(D) = (g_{ij}(D))$ is reduced
- The matrix of highest coefficients G^{hc} has rank k

$$G^{hc} = \underset{D^{\nu_i}}{\text{coefficient}}\; g_{ij}(D)\ , \qquad \nu_i \text{ the } i\text{-th row degree of } G(D)'s$$

- $G(D)$ has the predictable degree property : For any $u(D) = (u_1(D), u_2(D), \dots, u_k(D))$

$$\deg(u(D)G(D)) = \max_{1 \le i \le k} (\deg(u_i(D)) + \deg((g_{i1}(D), \dots, g_{in}(D)))$$

- Internal degree $G(D)$ = External degree $G(D)$

Example

$$\text{Is} \qquad G(D) = \begin{pmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{pmatrix} \qquad \text{basic?}$$

Yes. $G(0), G(1)$ have full rank. Is it reduced?

$$G^{hc} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ is not full rank} \to \text{it is not reduced.}$$

The equivalent encoder $\overline{G}(D)$

$$\overline{G}(D) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{pmatrix}$$

is reduced!

Example

$$\text{Is} \qquad G(D) = \begin{pmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{pmatrix} \qquad \text{basic?}$$

Yes. $G(0), G(1)$ have full rank. Is it reduced?

$$G^{hc} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ is not full rank} \rightarrow \text{it is not reduced.}$$

The equivalent encoder $\overline{G}(D)$

$$\overline{G}(D) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{pmatrix}$$

is reduced!

Theorem

If $G(D)$ is a basic reduced generator matrix for $\mathcal{C}$ (minimal), then

$$\textit{Internal degree}G(D) = \textit{External degree}G(D) =: \textit{deg}\,\mathcal{C}$$

Catastrophic Encoders

An information word u(D) is encoded into the codeword

$$v(D) = u(D)G(D),$$

and $v(D)$ is then transmitted over a noisy channel and received as $y(D)$. The decoder:

1. "hard" job": find a codeword, say $\hat{v}(D)$, which is "close" to $y(D)$
2. "easy" job": calculate the information word $\hat{u}(D)$ corresponding to $\hat{v}(D)$ but here catastrophes can occur!!

Catastrophe occurs when the codeword error has finite weight but the corresponding information error has infinite weight.

Definition

$G(D)$ is catastrophic if there is an infinite-weight vector $u(D)$ such that $v(D) = u(D)G(D)$ has finite weight.

Theorem (Massey)

The following are equivalent:

- $G(D)$ is noncatastrophic
- The gcd of the $k \times k$ minors of $G(D)$ is a power of D
- $G(D)$ has a right *finite weight* inverse

Example

The encoder

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

is noncatastrophic as an inverse is

$$H(D) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ D^{-1} & 1+D^{-1} \end{pmatrix}$$

Historical Remarks

- Convolutional codes were introduced by Elias (1955)
- The theory was imperfectly understood until a series of papers of Forney in the 70's on the algebra of the $k \times n$ matrices over the field of rational functions in the delay operator D.
- Became widespread in practice with the Viterbi decoding. In fact, they belong to the most widely implemented codes in (wireless) communications. The field is typically $\mathbb{F}_2$ and the rate and degree are small so that the Viterbi decoding algorithm is efficient.
- Recursive systematic convolutional codes were invented by Claude Berrou around 1991: turbo codes.
- Widely used in digital video, radio, mobile communications and satellite communications. Also used in the Voyager program (NASA).
- In the last decade a renewed interest has grown for convolutional codes over large fields trying to fully exploit the potential of convolutional codes.

References

G.D. Forney, Jr. (1975)
"Minimal bases of rational vector spaces, with applications to multivariable linear systems",
SIAM J. Control 13, 493–520, 1975.

G.D. Forney, Jr. (1970)
"Convolutional codes I: algebraic structure ",
IEEE Trans. Inform. Theory vol. IT-16, pp. 720-738, 1970.

R.J. McEliece (1998)
The Algebraic Theory of Convolutional Codes
Handbook of Coding Theory Vol. 1 , North-Holland, Amsterdam.

Johannesson, Rolf and Zigangirov, K. (1998, 2015)
Fundamentals of convolutional coding
IEEE Communications society and IEEE Information theory society and Vehicular Technology Society.

Summary of the basics

- Convolutional codes are block codes with memory
- They can be represented by polynomial matrices and state space representations
- We have studied several properties of polynomial matrices: Basic, reduced and catastrophic

Exercise 1

The following encoder

$$G(D) = \begin{pmatrix} 1+D & 0 & 1 & D \\ D & 1+D+D^2 & D^2 & 1 \end{pmatrix}$$

- is basic?
- is reduced?
- Find an equivalent basic and reduced (minimal) encoder.
- Encode the information sequence

$$10\ 00\ 01\ 11$$

Exercise 2

Build a shift register of the following encoder

$$\begin{pmatrix} 1+D+D^2 & 1+D^3 \end{pmatrix}$$

Encode the information sequence 0 0 0 1 0 1.