MDP Convolutional Codes

Thurnau, April 13, 2010

Joachim Rosenthal

Rosenthal@math.uzh.ch

Department of Mathematics
University of Zürich

Outline of Talk:

1. Convolutional Codes, Basics
2. MDS Convolutional Codes
3. MDP Convolutional Codes
4. Superregular Matrices
5. Decoding over the Erasure Channel

1. Convolutional Codes, Basics

Definition. Let $\mathbb{F}$ be a finite field. $R = \mathbb{F}[z]$ the polynomial ring. A submodule $\mathcal{C} \subset R^n$ is called a convolutional code.

1. Convolutional Codes, Basics

Definition. Let $\mathbb{F}$ be a finite field. $R = \mathbb{F}[z]$ the polynomial ring. A submodule $\mathcal{C} \subset R^n$ is called a convolutional code.

Since R is a principal ideal domain, the submodule $\mathcal{C}$ is free and there exists a $n \times k$ matrix $G(z)$ such that:

$$\mathcal{C} = \{G(z)m(z) \mid m(z) \in \mathbb{F}^k[z] = R^k\}$$

We call $G(z)$ a generator matrix of the code $\mathcal{C}$ and one says $\mathcal{C}$ has *rate* k/n.

1. Convolutional Codes, Basics

Definition. Let $\mathbb{F}$ be a finite field. $R = \mathbb{F}[z]$ the polynomial ring. A submodule $\mathcal{C} \subset R^n$ is called a convolutional code.

Since R is a principal ideal domain, the submodule $\mathcal{C}$ is free and there exists a $n \times k$ matrix $G(z)$ such that:

$$\mathcal{C} = \{G(z)m(z) \mid m(z) \in \mathbb{F}^k[z] = R^k\}$$

We call $G(z)$ a generator matrix of the code $\mathcal{C}$ and one says $\mathcal{C}$ has *rate* k/n.

Without loss of generality one can assume that a generator matrix is column reduced having column degrees $\delta_1, \ldots, \delta_k$.

Basics

Two $n \times k$ generator matrices $G(z)$ and $\tilde{G}(z)$ define the same code if and only if there is a $k \times k$ unimodular matrix $U(z)$ such that

$$\tilde{G}(z) = G(z)U(z).$$

Basics

Two $n \times k$ generator matrices $G(z)$ and $\tilde{G}(z)$ define the same code if and only if there is a $k \times k$ unimodular matrix $U(z)$ such that

$$\tilde{G}(z) = G(z)U(z).$$

Definition. The largest degree of the $k \times k$ fullsize minors of $G(z)$ is called the degree δ of the code.

Basics

Two $n \times k$ generator matrices $G(z)$ and $\tilde{G}(z)$ define the same code if and only if there is a $k \times k$ unimodular matrix $U(z)$ such that

$$\tilde{G}(z) = G(z)U(z).$$

Definition. The largest degree of the $k \times k$ fullsize minors of $G(z)$ is called the degree δ of the code.

Remark. The degree is a code parameter and is also equal to the sum of the column degrees: $\delta = \sum_{i=1}^{k} \delta_i$.

Basics

Two $n \times k$ generator matrices $G(z)$ and $\tilde{G}(z)$ define the same code if and only if there is a $k \times k$ unimodular matrix $U(z)$ such that

$$\tilde{G}(z) = G(z)U(z).$$

Definition. The largest degree of the $k \times k$ fullsize minors of $G(z)$ is called the degree δ of the code.

Remark. The degree is a code parameter and is also equal to the sum of the column degrees: $\delta = \sum_{i=1}^{k} \delta_i$.

It is a major design problem to construct (n,k,δ) codes, i.e. codes having a rate k/n and degree δ such that the code has “good parameters”.

Parity Check Matrix

Definition. A code $\mathcal{C}$ is called *observable* or *non-catastrophic* if one and hence every generator matrix $G(z)$ of $\mathcal{C}$ is right-prime.

Parity Check Matrix

Definition. A code $\mathcal{C}$ is called *observable* or *non-catastrophic* if one and hence every generator matrix $G(z)$ of $\mathcal{C}$ is right-prime.

Theorem. *If $\mathcal{C}$ is an observable (n,k,δ) code, then there exists an $(n-k)\times n$ parity check matrix $H(z)$ such that $\mathcal{C}$ is equivalently described through*

$$\mathcal{C} = \{v(z) \in \mathbb{F}^n[z] \mid H(z)v(z) = 0.\}$$

Historical Remarks

Convolutional Codes were introduced by Elias (1955). For this consider an $[n,k]$ linear block code represented by an $n \times k$ generator matrix G,

Historical Remarks

Convolutional Codes were introduced by Elias (1955). For this consider an $[n,k]$ linear block code represented by an $n \times k$ generator matrix G,

If messages $m_0, m_1, \ldots, m_N \in \mathbb{F}^k$ have to be encoded define:

$$m(z) = m_0 + m_1 z + \cdots + m_N z^N \in \mathbb{F}^k[z].$$

The encoding is then represented by

$$v(z) = Gm(z) \in \mathbb{F}^n[z]$$

Historical Remarks

Convolutional Codes were introduced by Elias (1955). For this consider an $[n,k]$ linear block code represented by an $n \times k$ generator matrix G,

If messages $m_0, m_1, \ldots, m_N \in \mathbb{F}^k$ have to be encoded define:

$$m(z) = m_0 + m_1 z + \cdots + m_N z^N \in \mathbb{F}^k[z].$$

The encoding is then represented by

$$v(z) = Gm(z) \in \mathbb{F}^n[z]$$

It was the idea of Elias to allow polynomial matrices $G(z)$ in the encoding process. Convolutional codes generalize block codes in a natural way.

Engineering Remarks

- Convolutional codes belong to the most widely implemented codes in (wireless) communications. The field is typically $\mathbb{F}_2$ and the rate and the degree are often small. The degree is small so that the Viterbi decoding algorithm is efficient.

Engineering Remarks

- Convolutional codes belong to the most widely implemented codes in (wireless) communications. The field is typically $\mathbb{F}_2$ and the rate and the degree are often small. The degree is small so that the Viterbi decoding algorithm is efficient.

- In recent work by Hadjicostis and Verghese [HV02] Convolutional codes over large alphabets were used in order to construct fault tolerant finite state machines.

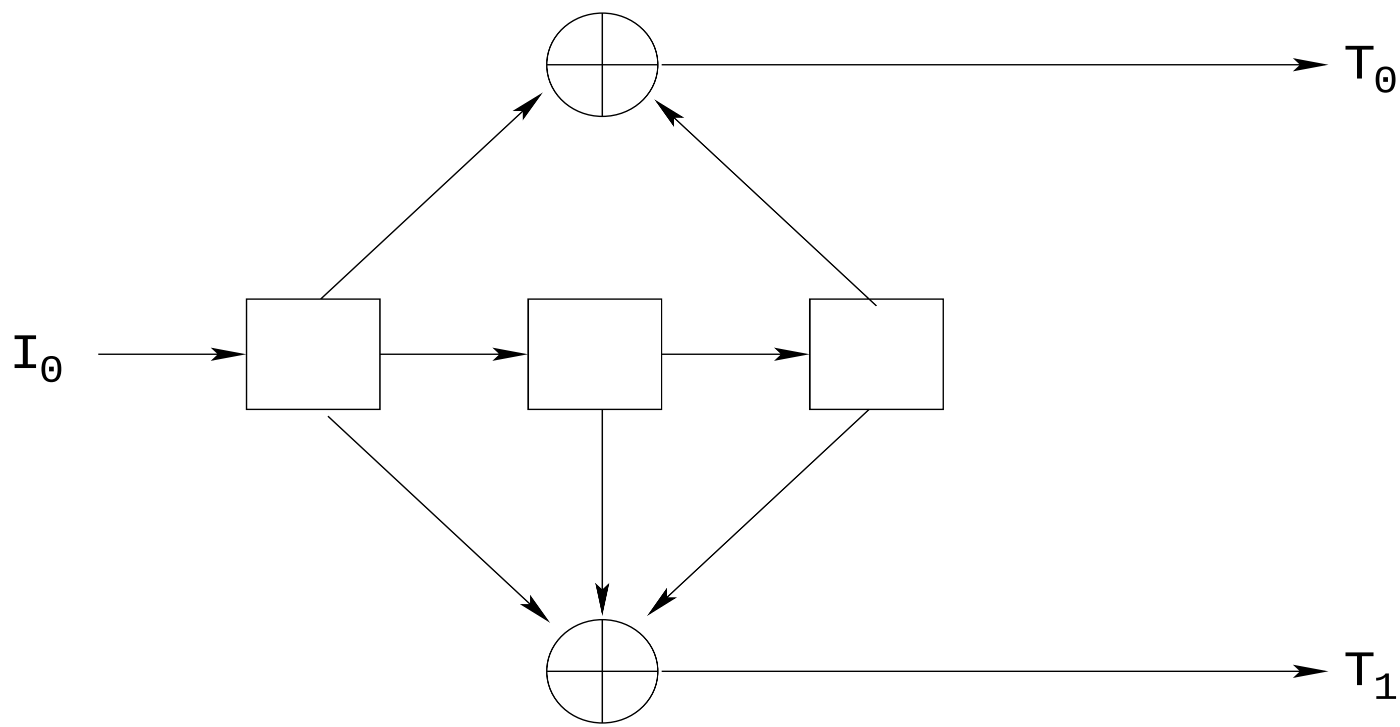
Engineering Remarks

- Convolutional codes belong to the most widely implemented codes in (wireless) communications. The field is typically $\mathbb{F}_2$ and the rate and the degree are often small. The degree is small so that the Viterbi decoding algorithm is efficient.
- In recent work by Hadjicostis and Verghese [HV02] Convolutional codes over large alphabets were used in order to construct fault tolerant finite state machines.
- In collaboration with Tomas and Smarandache [TRS09] we showed that in packet switched networks (like e.g. the Internet) convolutional codes over large alphabets have a lot of potentials.

Feed Forward Implementation

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

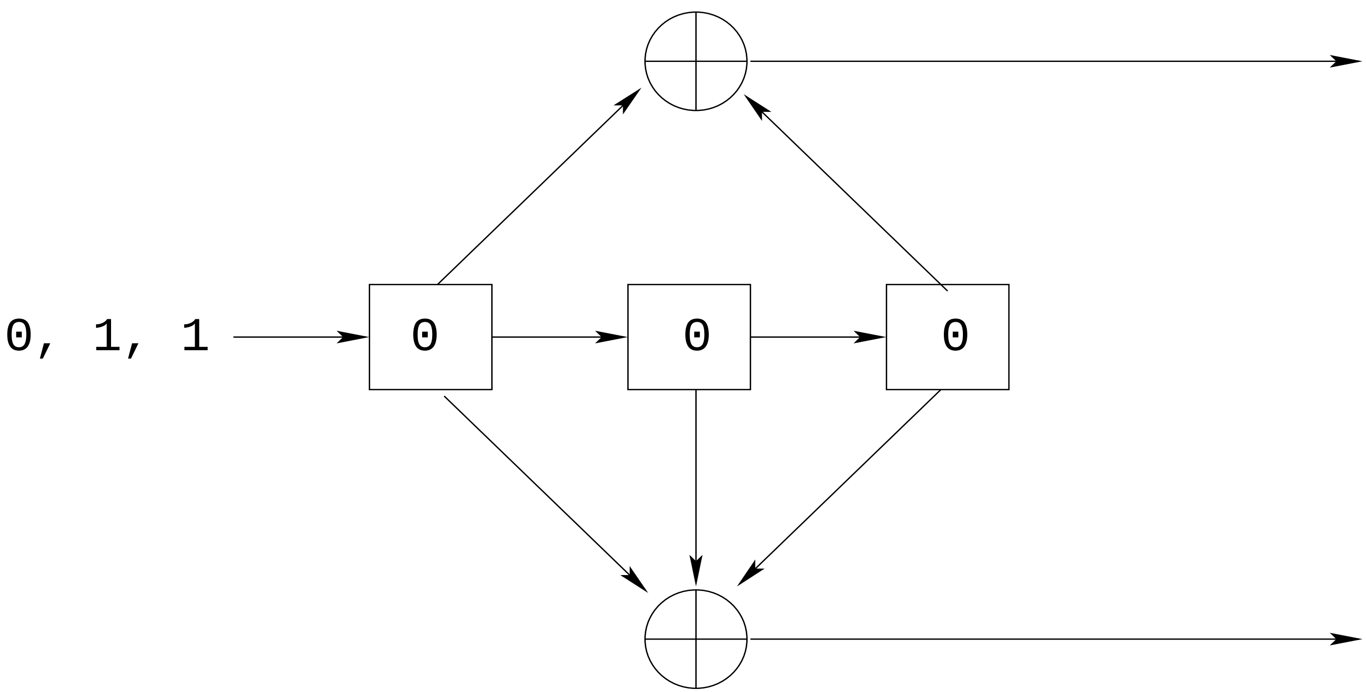
has the implementation:



Feed Forward Implementation

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

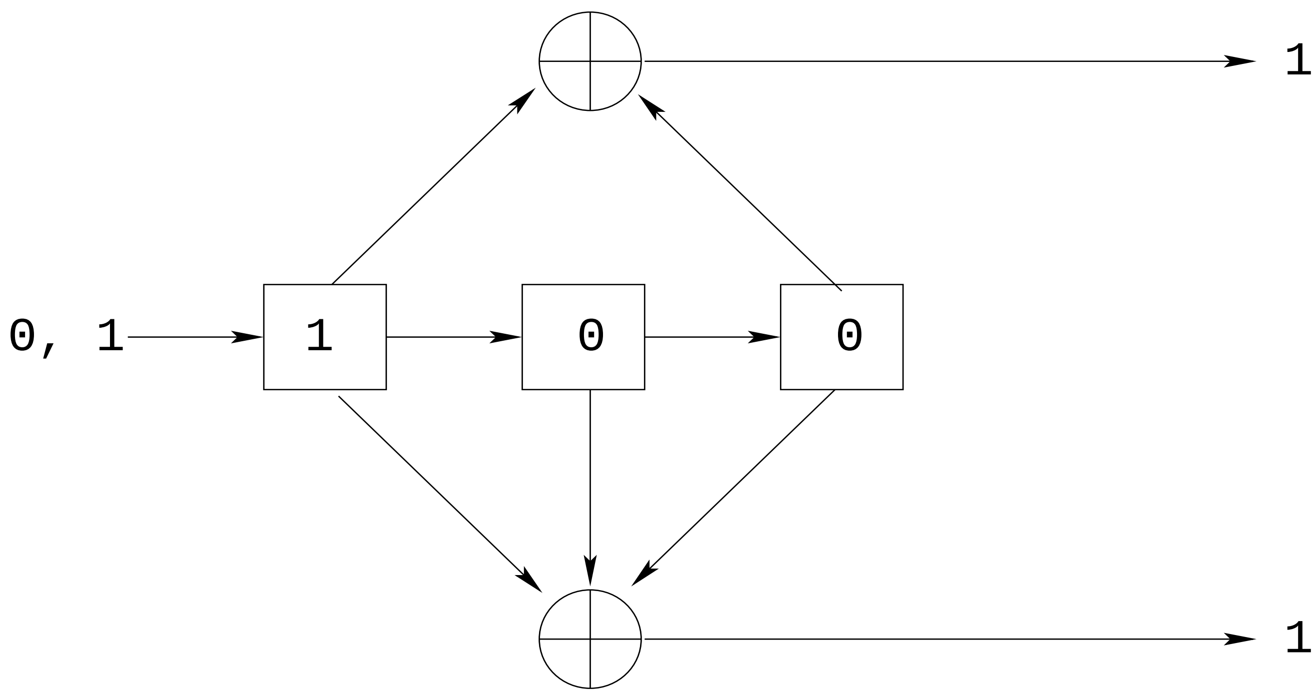
has the implementation:



Feed Forward Implementation

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

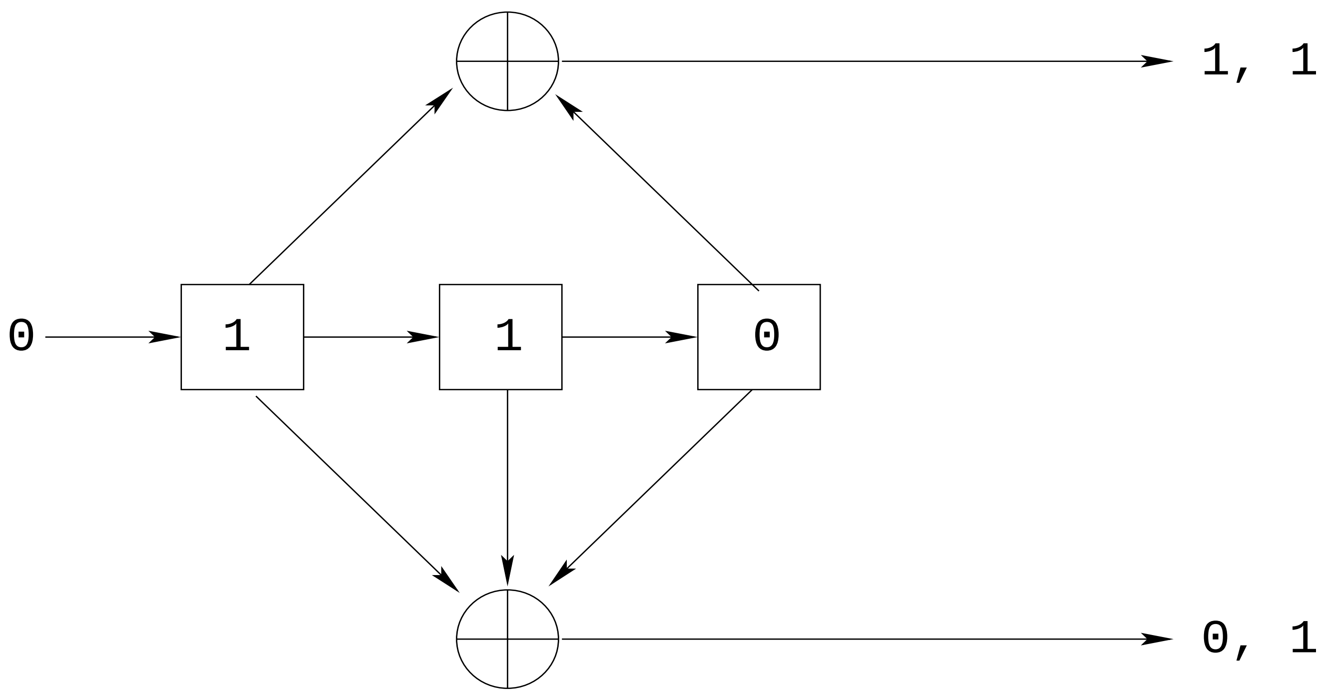
has the implementation:



Feed Forward Implementation

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

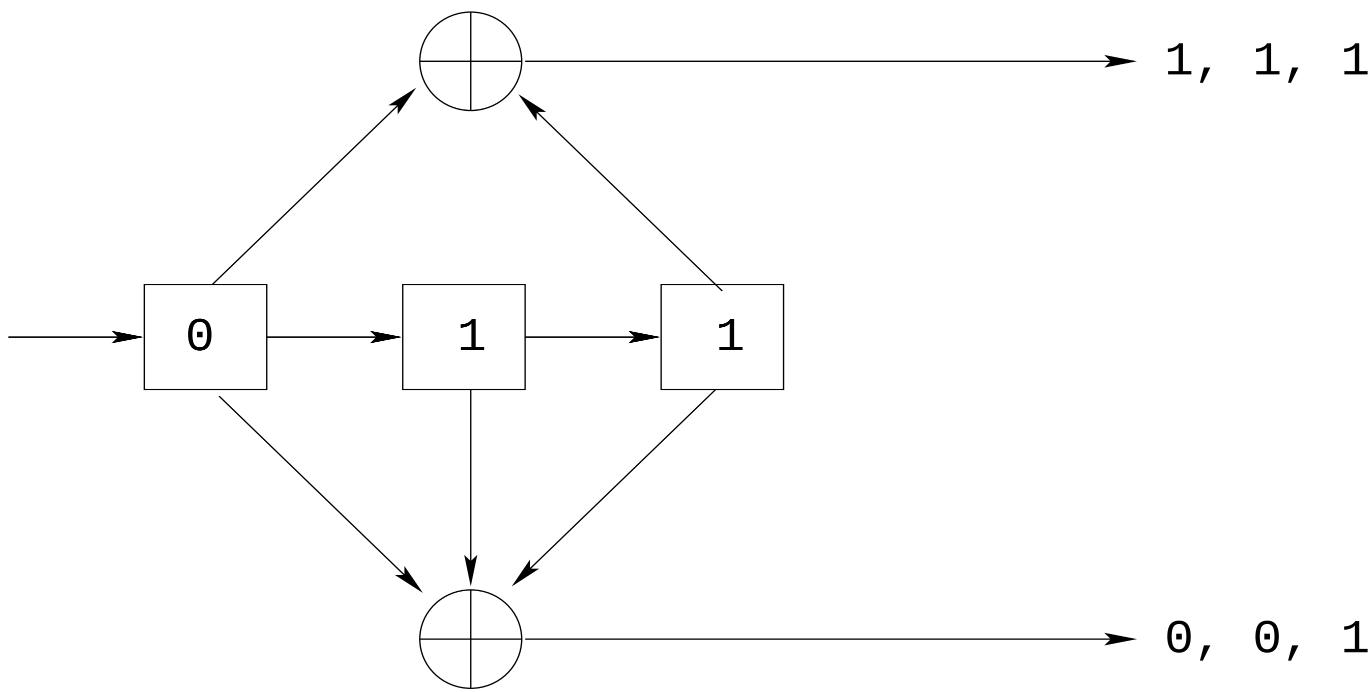
has the implementation:



Feed Forward Implementation

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

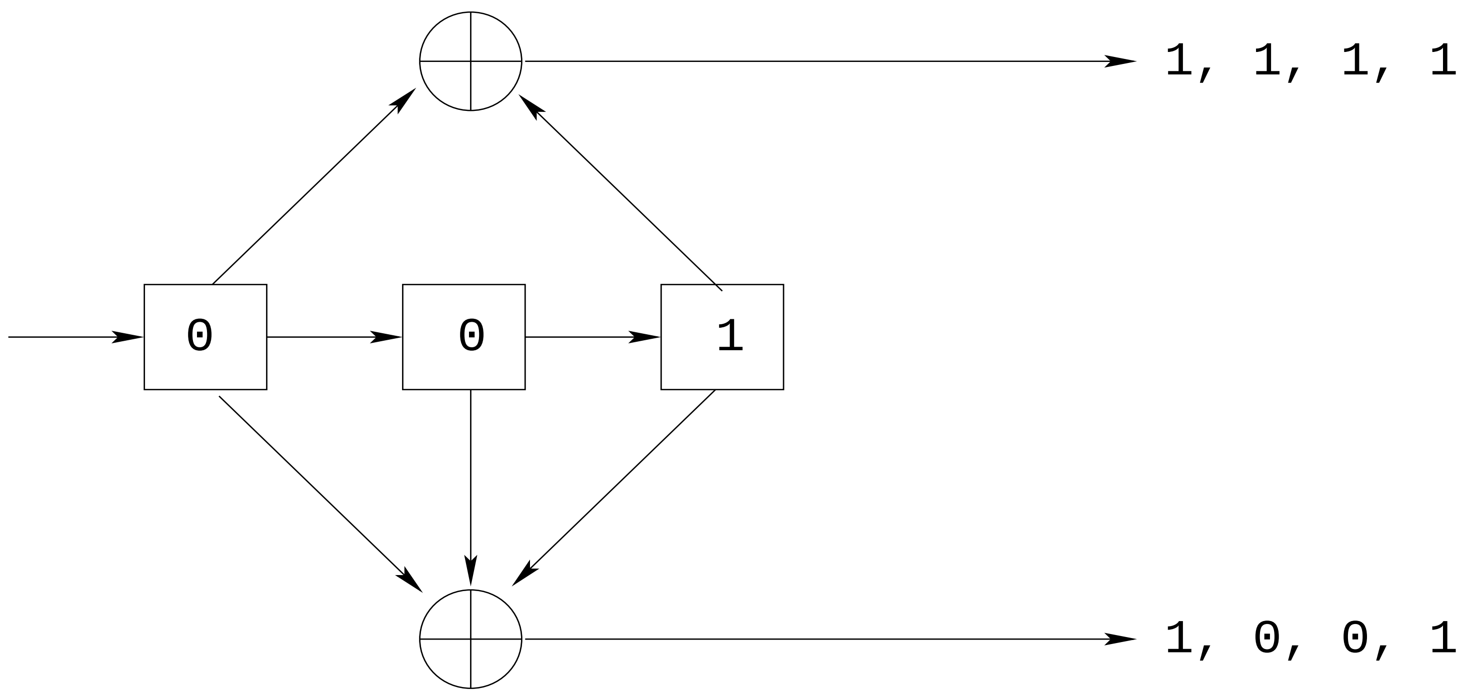
has the implementation:



Feed Forward Implementation

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

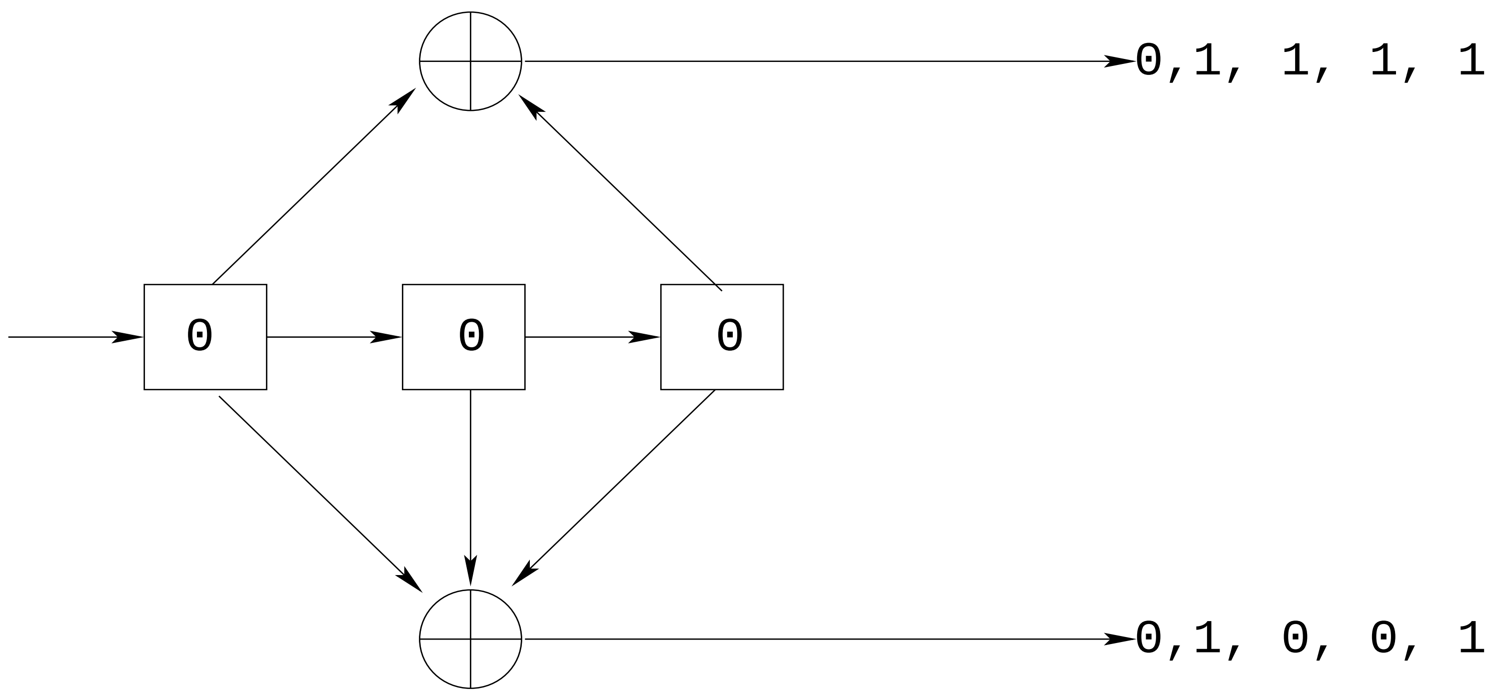
has the implementation:



Feed Forward Implementation

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

has the implementation:



Mathematical Remarks

- A convolutional code $\mathcal{C}$ defines also a rational map

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathrm{Grass}(k, \mathbb{F}^n) \\ z & \longmapsto & \mathrm{colsp}_{\mathbb{F}}(G(z)). \end{array}$$

Mathematical Remarks

- A convolutional code $\mathcal{C}$ defines also a rational map

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathrm{Grass}(k, \mathbb{F}^n) \\ z & \longmapsto & \mathrm{colsp}_{\mathbb{F}}(G(z)). \end{array}$$

- Alternatively one has an associated quotient sheaf.

Mathematical Remarks

- A convolutional code $\mathcal{C}$ defines also a rational map

$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathrm{Grass}(k,\mathbb{F}^n) \\ z & \longmapsto & \mathrm{colsp}_{\mathbb{F}}(G(z)). \end{array}$$

- Alternatively one has an associated quotient sheaf.
- The degree of the rational map corresponds to the degree of the convolutional code. The column degrees correspond to the Grothendieck indices and the set of all (n,k,δ) convolutional codes is parameterized by Grothendieck's Quot Scheme $Q^{\delta}_{k,n}$.

Connection to Systems Theory

It follows e.g. from the Hermann-Martin identification that every convolutional code can also be represented by a linear system. In particular for every (n,k,δ) code there exist matrices $A \in \mathbb{F}^{\delta\times\delta}$, $B \in \mathbb{F}^{\delta\times k}$, $C \in \mathbb{F}^{(n-k)\times\delta}$, and $D \in \mathbb{F}^{(n-k)\times k}$.
The rate k/n convolutional code $\mathcal{C}$ is then described by the linear system of (McMillan) degree δ:

$$\begin{aligned} x_{t+1} &= Ax_t + Bu_t, \\ y_t &= Cx_t + Du_t, \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix},\ x_0 = 0. \end{aligned} \tag{1}$$

2. MDS Convolutional Codes

Definition. If $v(z) = v_0 + v_1 z + \cdots + v_N z^N \in \mathbb{F}^n[z]$ one defines the *weight* of $v(z)$ through:

$$\mathrm{wt}\,(v(z)) := \sum_{i=0}^{N} \mathrm{wt}\,(v_i).$$

2. MDS Convolutional Codes

Definition. If $v(z) = v_0 + v_1 z + \cdots + v_N z^N \in \mathbb{F}^n[z]$ one defines the *weight* of $v(z)$ through:

$$\mathrm{wt}\,(v(z)) := \sum_{i=0}^{N} \mathrm{wt}\,(v_i).$$

If $v(z), \tilde{v}(z) \in \mathbb{F}^n[z]$ one defines the Hamming distance through:

$$\mathrm{Ham}\,((v(z), \tilde{v}(z))) := \mathrm{wt}\,(v(z) - \tilde{v}(z)).$$

2. MDS Convolutional Codes

Definition. If $v(z) = v_0 + v_1 z + \cdots + v_N z^N \in \mathbb{F}^n[z]$ one defines the *weight* of $v(z)$ through:

$$\mathrm{wt}\,(v(z)) := \sum_{i=0}^{N} \mathrm{wt}\,(v_i).$$

If $v(z), \tilde{v}(z) \in \mathbb{F}^n[z]$ one defines the Hamming distance through:

$$\mathrm{Ham}\,((v(z), \tilde{v}(z))) := \mathrm{wt}\,(v(z) - \tilde{v}(z)).$$

For a convolutional code $\mathcal{C}$ one defines the *free distance*

$$d_{\mathrm{free}} := \min_{\substack{u,v \in \mathcal{C} \\ u \neq v}} \mathrm{Ham}\,(u(z), v(z))\,. \tag{4}$$

Remark

For fixed values δ, k, n we are interested in the maximum possible value of

$$d_{free}: \; Q^{\delta}_{k,n}(\mathbb{F}) \longrightarrow \mathbb{N} = \{1,2,3,\ldots\}$$

For $\delta = 0$ we know that the maximum value is given by the Singleton bound:

$$n - k + 1$$

and this value is attained if $|\mathbb{F}| > n$.

Examples:

Example.

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

defines a binary rate 1/2 convolutional code of degree $\delta = 2$ and distance $d_{\text{free}} = 5$.

Examples:

Example.

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

defines a binary rate 1/2 convolutional code of degree $\delta = 2$ and distance $d_{\text{free}} = 5$.

Example. Let $\mathbb{F} = \mathbb{F}_7$, the prime field of 7 elements.

$$G(z) = \begin{pmatrix} z^3+2z+5 & 0 \\ 5z^3+3 & 1 \\ z^2+5 & 2 \\ 2z+5 & 3 \end{pmatrix},$$

defines a convolutional code of rate $k/n = 2/4$, degree $\delta = 3$ and free distance $d_0 = d_{\text{free}} = 3$.

Generalized Singleton Bound

Lemma ([RS99])**.** *The free distance of an* (n,k,δ)*-code satisfies*

$$d_{\text{free}} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{5}$$

Generalized Singleton Bound

Lemma ([RS99])**.** *The free distance of an* (n,k,δ)*-code satisfies*

$$d_{\text{free}} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{6}$$

The bound on the right hand side is called the *generalized Singleton bound*. Codes attaining this bound are called MDS convolutional codes.

Generalized Singleton Bound

Lemma ([RS99])**.** *The free distance of an* (n,k,δ)*-code satisfies*

$$d_{\text{free}} \le (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{7}$$

The bound on the right hand side is called the *generalized Singleton bound*. Codes attaining this bound are called MDS convolutional codes.

Theorem ([RS99])**.** *For every* (n,k,δ) *there exist MDS convolutional codes over sufficiciently large fields.*

Generalized Singleton Bound

Lemma ([RS99])**.** *The free distance of an* (n, k, δ)*-code satisfies*

$$d_{\text{free}} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{8}$$

The bound on the right hand side is called the *generalized Singleton bound*. Codes attaining this bound are called MDS convolutional codes.

Theorem ([RS99])**.** *For every* (n, k, δ) *there exist MDS convolutional codes over sufficiciently large fields.*

Remark. The original proof [RS99] was non-constructive and it showed that MDS convolutional codes are Zariski dense in Grothedieck's Quot Scheme $Q^{\delta}_{k,n}$.

Remarks:

- For $\delta = 0$ the upper bound (5) reduces to the block code situation:

$$d_{\text{free}} \leq n - k + 1.$$

Remarks:

- For $\delta = 0$ the upper bound (5) reduces to the block code situation:

$$d_{\text{free}} \leq n - k + 1.$$

- If $k = 1$ the upper bound (5) reduces to

$$d_{\text{free}} \leq n(\delta + 1).$$

This situation was studied by Justesen [Jus75].

3. MDP Convolutional Codes

Definition. The jth column distance of the code $\mathcal{C}$ is defined as

$$d_j := \min\left\{ \sum_{t=0}^{j} \mathrm{wt}\,(v_t) \mid \sum_{t=0}^{N} v_t z^t \in \mathcal{C}, v_0 \neq 0 \right\}.$$

3. MDP Convolutional Codes

Definition. The jth column distance of the code $\mathcal{C}$ is defined as

$$d_j := \min\left\{ \sum_{t=0}^{j} \mathrm{wt}\left(v_t\right) \mid \sum_{t=0}^{N} v_t z^t \in \mathcal{C}, v_0 \neq 0 \right\}.$$

One has that $d_0 \leq d_1 \leq d_2 \leq \ldots$.

3. MDP Convolutional Codes

Definition. The jth column distance of the code $\mathcal{C}$ is defined as

$$d_j := \min \left\{ \sum_{t=0}^{j} \mathrm{wt}(v_t) \mid \sum_{t=0}^{N} v_t z^t \in \mathcal{C}, v_0 \neq 0 \right\}.$$

One has that $d_0 \leq d_1 \leq d_2 \leq \ldots$.
The Free distance is also equal to:

$$d_{\mathrm{free}} = \lim_{j \to \infty} d_j \tag{11}$$

Bound on Column Distance Indices

Lemma. *[GLRS06] For every* $j \in \mathbb{N}_0$ *we have*

$$d_j \leq (n-k)(j+1)+1.$$

Bound on Column Distance Indices

Lemma. *[GLRS06] For every $j \in \mathbb{N}_0$ we have*

$$d_j \leq (n-k)(j+1)+1.$$

$\mathcal{C}$ is said to have a *maximum distance profile* if

$$d_j = (n-k)(j+1)+1 \text{ for } j = 0,\ldots,L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor.$$

Bound on Column Distance Indices

Lemma. *[GLRS06] For every $j \in \mathbb{N}_0$ we have*

$$d_j \leq (n-k)(j+1)+1.$$

$\mathcal{C}$ is said to have a *maximum distance profile* if

$$d_j = (n-k)(j+1)+1 \text{ for } j = 0,\ldots,L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor.$$

Theorem ([HRS05])**.** *For integers n,k,δ and for sufficiently large fields the set of maximum distance profile codes forms a Zariski dense subset of Grothendieck's Quot Scheme $Q^{\delta}_{k,n}$.*

Example

Example. Let

$$G(z) = \begin{pmatrix} (z-1) & 1 \\ (z-2) & 1 \\ (2z-3) & 1 \end{pmatrix}$$

be an encoder for a rate $2/3$ convolutional code $\mathcal{C}$ of degree $\delta = 1$, over $\mathbb{F}_5$. The encoder is non-catastrophic. The generalized Singleton bound gives $d_{\text{free}} \leq 3$.
One shows that the code has $d_{\text{free}} = 3$, hence is a MDS code. The code has maximum distance profile as $d_0 = 2$ and $d_1 = d_{\text{free}} = 3$.

Algebraic Characterization

Assume that the parity check matrix is given as $H(z) = \sum_{i=0}^{\nu} H_i z^i$.
For each $j > \nu$ let $H_j = 0$ and define:

$$\mathcal{H}_j = \begin{pmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{pmatrix} \in \mathbb{F}^{(j+1)(n-k)\times(j+1)n}. \qquad (12)$$

Algebraic Characterization

Assume that the parity check matrix is given as $H(z) = \sum_{i=0}^{\nu} H_i z^i$. For each $j > \nu$ let $H_j = 0$ and define:

$$\mathcal{H}_j = \begin{pmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{pmatrix} \in \mathbb{F}^{(j+1)(n-k)\times(j+1)n}. \tag{13}$$

Theorem. *([GLRS06, Proposition 2.1]) Let $d \in \mathbb{N}$. The following properties are equivalent.*

1. *$d_j^c = d$;*
2. *none of the first n columns of $\mathcal{H}_j$ is contained in the span of any other $d-2$ columns and one of the first n columns of $\mathcal{H}_j$ is in the span of some other $d-1$ columns of that matrix.*

4. Superregular Matrices

Definition. Let A be an $n \times n$ lower triangular Toeplitz matrix and let $A^{i_1,\dots,i_r}_{j_1,\dots,j_r}$ be the submatrix obtained from A by picking the rows with indices $i_1,\dots,i_r$ and columns $j_1,\dots,j_r$.
A is called *superregular* if every submatrix $A^{i_1,\dots,i_r}_{j_1,\dots,j_r}$ is nonsingular for every $1 \le r \le n$ and every $i_1,\dots,i_r, j_1,\dots,j_r$ with $j_\nu \le i_\nu$.

4. Superregular Matrices

Definition. Let A be an $n \times n$ lower triangular Toeplitz matrix and let $A^{i_1,\dots,i_r}_{j_1,\dots,j_r}$ be the submatrix obtained from A by picking the rows with indices $i_1,\dots,i_r$ and columns $j_1,\dots,j_r$.
A is called *superregular* if every submatrix $A^{i_1,\dots,i_r}_{j_1,\dots,j_r}$ is nonsingular for every $1 \le r \le n$ and every $i_1,\dots,i_r, j_1,\dots,j_r$ with $j_\nu \le i_\nu$.

Remark. For rate $1/2$ codes the construction of supperregular matrices is essentially equivalent to the construction of MDP convolutional codes.

Example. For $n = 3$ and $\mathbb{F} = \mathbb{F}_3$ the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix}$$

is superregular. For $n = 5$ and $\mathbb{F} = \mathbb{F}_7$ the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 6 & 1 & 2 & 1 & 0 \\ 4 & 6 & 1 & 2 & 1 \end{bmatrix} \text{ is superregular.}$$

Using a computer algebra program one checks that the following matrices are superregular.

$$\begin{bmatrix} 1 & & & & \\ \beta & 1 & & & \\ \beta^3 & \beta & 1 & & \\ \beta & \beta^3 & \beta & 1 & \\ 1 & \beta & \beta^3 & \beta & 1 \end{bmatrix} \in \mathbb{F}_{2^3}^{5\times 5}, \begin{bmatrix} 1 & & & & & \\ \gamma & 1 & & & & \\ \gamma^5 & \gamma & 1 & & & \\ \gamma^5 & \gamma^5 & \gamma & 1 & & \\ \gamma & \gamma^5 & \gamma^5 & \gamma & 1 & \\ 1 & \gamma & \gamma^5 & \gamma^5 & \gamma & 1 \end{bmatrix} \in \mathbb{F}_{2^4}^{6\times 6},$$

where

$$\beta^3+\beta+1=0, \text{ and } \gamma^4+\gamma+1=0,$$

Example

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega^9 & \omega & 1 & 0 & 0 & 0 & 0 & 0 \\ \omega^{33} & \omega^9 & \omega & 1 & 0 & 0 & 0 & 0 \\ \omega^{33} & \omega^{33} & \omega^9 & \omega & 1 & 0 & 0 & 0 \\ \omega^9 & \omega^{33} & \omega^{33} & \omega^9 & \omega & 1 & 0 & 0 \\ \omega & \omega^9 & \omega^{33} & \omega^{33} & \omega^9 & \omega & 1 & 0 \\ 1 & \omega & \omega^9 & \omega^{33} & \omega^{33} & \omega^9 & \omega & 1 \end{bmatrix} \in \mathbb{F}_{2^6}^{8\times 8}.$$

where

$$\omega^6 + \omega + 1 = 0.$$

Proof of Existence

Example. Let the matrix X be equal to

$$X = \begin{bmatrix} 1 & & & & & \\ 1 & 1 & & & & \\ & 1 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & 1 & 1 & \\ & & & & 1 & 1 \end{bmatrix}. \tag{14}$$

Then

$$A = X^{n-1} = \begin{bmatrix} 1 & & & & & \\ n & 1 & & & & \\ \binom{n}{2} & n & 1 & & & \\ \vdots & \vdots & \ddots & \ddots & & \\ \binom{n}{n-1} & \binom{n}{n-2} & \dots & n & 1 & \\ 1 & \binom{n}{n-1} & \dots & & n & 1 \end{bmatrix} \tag{15}$$

is *totally positive* over the reals and superregular for sufficiently large prime fields.

Consequence

For every size n there exist superregular matrices over sufficiently large field sizes.

Consequence

For every size n there exist superregular matrices over sufficiently large field sizes.

On the side of the presented existence result we do not have good algebraic construction of superregular matrices. - Come up with constructions!

5. Decoding over the Erasure Channel:

Definition. The Erasure channel is a communication channel, where symbols either arrive correctly or the receiver knows that they are in error (or did not arrive at all).

5. Decoding over the Erasure Channel:

Definition. The Erasure channel is a communication channel, where symbols either arrive correctly or the receiver knows that they are in error (or did not arrive at all).

Remark: The Internet can be viewed as an erassure channel

5. Decoding over the Erasure Channel:

Definition. The Erasure channel is a communication channel, where symbols either arrive correctly or the receiver knows that they are in error (or did not arrive at all).

Remark: The Internet can be viewed as an erassure channel

Convolutional codes over any size alphabet have a polynomial time decoding algorithm over the erasure channel [TRS09]

Results:

Theorem. *Let* $\mathcal{C}$ *be an* (n,k,δ) *convolutional code with* $d^c_{j_0}$ *the* $j = j_0$*-th column distance. If in any sliding window of length* $(j_0+1)n$ *at most* $d^c_{j_0}-1$ *erasures occur then we can recover completely the transmited sequence.*

Results:

Theorem. *Let $\mathcal{C}$ be an (n,k,δ) convolutional code with $d^c_{j_0}$ the $j = j_0$-th column distance. If in any sliding window of length $(j_0+1)n$ at most $d^c_{j_0}-1$ erasures occur then we can recover completely the transmited sequence.*

The best scenario happens when the convolutional code is MDP. In this case full error correction 'from left to right' is possible as soon as the fraction of errasures is not more than $\frac{n-k}{n}$ in any sliding window of length $(L+1)n$.

Results:

Theorem. *Let $\mathcal{C}$ be an (n,k,δ) convolutional code with $d^c_{j_0}$ the $j = j_0$-th column distance. If in any sliding window of length $(j_0+1)n$ at most $d^c_{j_0}-1$ erasures occur then we can recover completely the transmited sequence.*

The best scenario happens when the convolutional code is MDP. In this case full error correction 'from left to right' is possible as soon as the fraction of errasures is not more than $\frac{n-k}{n}$ in any sliding window of length $(L+1)n$.

Corollary 3. *Let $\mathcal{C}$ be an (n,k,δ) MDP convolutional code. If in any sliding window of length $(L+1)n$ at most $(L+1)(n-k)$ erasures occur in a transmited sequence then we can completely recover the sequence in polynomial time in δ.*

Cmplete-MDP Convolutional Codes

Assume that $(n-k)\nu = \delta$, the degree of the code $\mathcal{C}$ and $\mathcal{C}$ has a parity check matrix $H(z) = H_0 + H_1 z + \cdots + H_\nu z^\nu$.

Cmplete-MDP Convolutional Codes

Assume that $(n-k)\nu = \delta$, the degree of the code $\mathcal{C}$ and $\mathcal{C}$ has a parity check matrix $H(z) = H_0 + H_1 z + \cdots + H_\nu z^\nu$.

Definition. A rate $\frac{k}{n}$ convolutional code $\mathcal{C}$ with parity check matrix $H(z)$ is called a *complete-MDP convolutional code* if in the $(L+1)(n-k) \times (\nu+L+1)n$ matrix

$$\begin{bmatrix} H_\nu & \cdots & H_0 & & & \\ & H_\nu & & H_0 & & \\ & & \ddots & & \ddots & \\ & & & H_\nu & \cdots & H_0 \end{bmatrix}$$

every full size minor which is not trivially zero, is nonzero.

Example

The following parity check matrix represents a $(3,1,1)$ complete-MDP convolutional code over $\mathbb{F}_{128}$ with $\alpha^7+\alpha^6+\alpha^3+\alpha+1=0$.

$$H(z)=\begin{bmatrix} \alpha^{76}+\alpha^{77}z & \alpha^{62}+\alpha^{85}z & 1+\alpha^{76}z \\ \alpha^{73}+\alpha^{37}z & \alpha^{76}+\alpha^{77}z & \alpha^{62}+\alpha^{85}z \end{bmatrix}.$$

The partial parity check matrix has all its full size minors that are not trivially zero nonzero. I.E. minors that don't include columns 1, 2 and 3 or 7, 8 and 9, are nonzero.

$$\begin{bmatrix} \alpha^{77} & \alpha^{85} & \alpha^{76} & \alpha^{76} & \alpha^{62} & 1 & & & \\ \alpha^{13} & \alpha^{77} & \alpha^{85} & \alpha^{73} & \alpha^{76} & \alpha^{82} & & & \\ & & & \alpha^{77} & \alpha^{85} & \alpha^{76} & \alpha^{76} & \alpha^{62} & 1 \\ & & & \alpha^{13} & \alpha^{77} & \alpha^{85} & \alpha^{73} & \alpha^{76} & \alpha^{82} \end{bmatrix}.$$

Results

Lemma. *Complete-MDP convolutional codes are MDP convolutional codes.*

Results

Lemma. *Complete-MDP convolutional codes are MDP convolutional codes.*

Theorem. *If in a window of size* $(\nu+L+1)n$ *there are not more than* $(L+1)(n-k)$ *erasures and they are distributed in such a way that between position* 1 *and* sn *and between positions* $(\nu+L+1)n$ *and* $(\nu+L+1)n-s(n-k)$*, for* $s=1,2,\ldots,L+1$*, there are not more than* $s(n-k)$ *erasures then full correction of all symbols in this interval will be possible.*

Conclusion

(1) Convolutional codes generalize linear block codes in a natural way.

(2) Convolutional codes capable of decoding a large number of errors per time interval require a large free distance and a good distance profile.

(3) Very few constructions for codes with large distance are known. **We do not have a general construction for complete MDP codes!**.

(4) Typically convolutional codes are decoded via the Viterbi decoding algorithm. The complexity of this algorithm grows exponentially with the McMillan degree. New classes of codes coming with more efficient decoding algorithms are needed.

References

[GLRS06] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, *Strongly MDS convolutional codes*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 584–598.

[GLS04] H. Gluesing-Luerssen and W. Schmale, *On cyclic convolutional codes*, Acta Appl. Math **82** (2004), 183–237.

[HRS05] R. Hutchinson, J. Rosenthal, and R. Smarandache, *Convolutional codes with maximum distance profile*, Systems & Control Letters **54** (2005), no. 1, 53–63.

[HV02] C. N. Hadjicostis and G. C. Verghese, *Encoded dynamics for fault tolerance in linear finite-state machines*, IEEE Trans. Automat. Contr. **47** (2002), no. 1, 189–192.

[Jus75] J. Justesen, *An algebraic construction of rate* $1/\nu$ *convolutional codes*, IEEE Trans. Inform. Theory **IT-21** (1975), no. 1, 577–580.

[JZ99] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of convolutional coding*, IEEE Press, New York, 1999.

[RS99] J. Rosenthal and R. Smarandache, *Maximum distance separable convolutional codes*, Appl. Algebra Engrg. Comm. Comput. **10** (1999), no. 1, 15–32.

[TRS09] V. Tomas, J. Rosenthal, and R. Smarandache, *Decoding of MDP convolutional codes over the erasure channel*, Proceedings of the 2009 IEEE

International Symposium on Information Theory (Seoul, South Korea), 2009, pp. 556–560.