Probability Estimates for Networks of Linear Systems over Finite Fields and Applications to Convolutional Codes

Julia Lieb

Institute of Mathematics, University of Würzburg

Networks of Linear Systems - a workshop in memory of U. Helmke and R. Kalman, Sde Boker, March 19-21, 2017

Linear Control Systems

For a field $\mathbb{F}$, let $A \in \mathbb{F}^{n\times n}, B \in \mathbb{F}^{n\times m}, C \in \mathbb{F}^{p\times n}, D \in \mathbb{F}^{p\times m}$. Consider a discrete-time linear control systems of the form

$$\begin{aligned} x(\tau+1) &= Ax(\tau) + Bu(\tau) \\ y(\tau) &= Cx(\tau) + Du(\tau) \end{aligned} \tag{1}$$

with input $u \in \mathbb{F}^m$, state vector $x \in \mathbb{F}^n$, output $y \in \mathbb{F}^p$ and $\tau \in \mathbb{N}_0$. One could identify this system with the matrix-quadruple (A, B, C, D).

Probability of Reachability

Let $\mathbb{F}$ be finite and endowed with the uniform probability distribution that assigns to each field element the same probability $t = \frac{1}{|\mathbb{F}|}$. Then, it holds:

Theorem (HJL 2014)

The probability that a pair $(A, B) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m}$, $n, m \in \mathbb{N}$ *is reachable is equal to*

$$P_{n,m}(t) := \prod_{j=m}^{n+m-1} (1 - t^j) = 1 - t^m + O(t^{m+1}).$$

HJL 2014: U. Helmke, J. Jordan and J. Lieb: Probability estimates for reachability of linear systems defined over finite fields, Advances in Mathematics of Communications, Vol. 10, No. 1(2016), 63-78.

Probability of Observability

Using that (A, C) is observable if and only if $(A^\top, C^\top)$ is reachable, one achieves:

Corollary

The probability that a pair $(A, C) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{p\times n}$, $n, p \in \mathbb{N}$ *is observable is equal to*

$$P_{n,p}(t) := \prod_{j=p}^{n+p-1} (1 - t^j) = 1 - t^p + O(t^{p+1}).$$

Probability of Reachability and Observability

Definition

Let $P^{rc}_{p,n,m}(t)$ be the probability that $P \in \mathbb{F}[z]^{p\times m}$ is right coprime with $Q \in \mathbb{F}[z]^{m\times m}$, where Q is in Kronecker-Hermite form with $\deg(\det(Q)) = n$ and $\deg_j P(z) \leq \deg_j Q(z)$ for $j = 1, ..., m$.

Probability of Reachability and Observability

Definition

Let $P^{rc}_{p,n,m}(t)$ be the probability that $P \in \mathbb{F}[z]^{p\times m}$ is right coprime with $Q \in \mathbb{F}[z]^{m\times m}$, where Q is in Kronecker-Hermite form with $\deg(\det(Q)) = n$ and $\deg_j P(z) \leq \deg_j Q(z)$ for $j = 1, ..., m$.

Proposition

The probability that $(A, B, C, D) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m} \times \mathbb{F}^{p\times n} \times \mathbb{F}^{p\times m}$ *with* $p, n, m \in \mathbb{N}$ *is reachable and observable is equal to*

$$P^{rc}_{p,n,m}(t) \cdot P_{n,m}(t)$$

Probability of Reachability and Observability

Definition

Let $P^{rc}_{p,n,m}(t)$ be the probability that $P \in \mathbb{F}[z]^{p\times m}$ is right coprime with $Q \in \mathbb{F}[z]^{m\times m}$, where Q is in Kronecker-Hermite form with $\deg(\det(Q)) = n$ and $\deg_j P(z) \leq \deg_j Q(z)$ for $j = 1, ..., m$.

Proposition

The probability that $(A, B, C, D) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m} \times \mathbb{F}^{p\times n} \times \mathbb{F}^{p\times m}$ *with* $p, n, m \in \mathbb{N}$ *is reachable and observable is equal to*

$$P^{rc}_{p,n,m}(t) \cdot P_{n,m}(t)$$

Idea of proof: Considering coprime factorization of the transfer function $T(z) = C(zI - A)^{-1}B + D = P(z)Q(z)^{-1}$.

Probability of Reachability and Observability

Theorem

$$P^{rc}_{p,n,m}(t) = 1 - t^p + O(t^{p+1})$$

Idea of proof:

- Consider Hermite and Kronecker-Hermite form
- Apply row and column operations
- Count polynomials whose values at some points are fixed

Corollary

The probability that $(A, B, C, D) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times m} \times \mathbb{F}^{p\times n} \times \mathbb{F}^{p\times m}$ *with* $p, n, m \in \mathbb{N}$ *is reachable and observable is equal to*

$$1 - t^m - t^p + O(t^{\min(m,p)+1}).$$

Networks of Linear Systems

Consider a **network** of N linear systems

$$\begin{aligned} x_i(\tau+1) &= A_i x_i(\tau) + B_i v_i(\tau) \\ w_i(\tau) &= C_i x_i(\tau) + D_i v_i(\tau) \\ v_i(\tau) &= \sum_{j=1}^{N} K_{ij} w_j(\tau) + L_i u(\tau) \\ y(\tau) &= \sum_{i=1}^{N} M_i w_i(\tau) + J u(\tau) \end{aligned}$$

with $A_i \in \mathbb{F}^{n_i \times n_i}$, $B_i \in \mathbb{F}^{n_i \times m_i}$, $C_i \in \mathbb{F}^{p_i \times n_i}$, $D_i \in \mathbb{F}^{p_i \times m_i}$, $K_{ij} \in \mathbb{F}^{m_i \times p_j}$, $L_i \in \mathbb{F}^{m_i \times m}$, $M_i \in \mathbb{F}^{p \times p_i}$ and $J \in \mathbb{F}^{p \times m}$.

Networks of Linear Systems

Define $K := (K_{ij})_{ij}$, $L := \begin{bmatrix} L_1 \\ \vdots \\ L_N \end{bmatrix}$ and $M := [M_1, \ldots, M_N]$,

$$A := \begin{bmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_N \end{bmatrix}, B := \begin{bmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_N \end{bmatrix},$$

$$C := \begin{bmatrix} C_1 & & 0 \\ & \ddots & \\ 0 & & C_N \end{bmatrix} \text{ and } D := \begin{bmatrix} D_1 & & 0 \\ & \ddots & \\ 0 & & D_N \end{bmatrix}.$$

Networks of Linear Systems

If $\det(I - DK) \neq 0$, this leads to the interconnected system

$$\begin{aligned} x(\tau + 1) &= \mathcal{A}x(\tau) + \mathcal{B}u(\tau) \\ y(\tau) &= \mathcal{C}x(\tau) + \mathcal{D}u(\tau), \end{aligned}$$

with

$$\begin{aligned} \mathcal{A} &= A + BK(I - DK)^{-1}C \\ \mathcal{B} &= BK(I - DK)^{-1}DL + BL = B(I - KD)^{-1}L \\ \mathcal{C} &= M(I - DK)^{-1}C \\ \mathcal{D} &= M(I - DK)^{-1}DL + J. \end{aligned}$$

Networks of Linear Systems

Theorem (FH 2015)

(A_i, B_i, C_i) reachable and observable for $i = 1, \ldots, N$

Coprime factorization: $C_i(zI - A_i)^{-1}B_i = P_i(z)Q_i(z)^{-1}$

$$Q(z) = \begin{bmatrix} Q_1(z) & & 0 \\ & \ddots & \\ 0 & & Q_N(z) \end{bmatrix}, \; P(z) = \begin{bmatrix} P_1(z) & & 0 \\ & \ddots & \\ 0 & & P_N(z) \end{bmatrix}$$

Then

$$(\mathcal{A}, \mathcal{B}) \text{ reachable} \;\Leftrightarrow\; (Q(z) - KP(z), L) \text{ left coprime}$$
$$(\mathcal{A}, \mathcal{C}) \text{ observable} \;\Leftrightarrow\; (Q(z) - KP(z), MP(z)) \text{ right coprime.}$$

FH 2015: P.A. Fuhrmann and U. Helmke: The mathematics of networks of linear systems, Springer, 2015.

Networks of Linear Systems

Theorem

(A_i, B_i, C_i, D_i) reachable and observable for $i = 1, \ldots, N$

Coprime factorization: $C_i(zI - A_i)^{-1}B_i + D_i = P_i(z)Q_i(z)^{-1}$

$$Q(z) = \begin{bmatrix} Q_1(z) & & 0 \\ & \ddots & \\ 0 & & Q_N(z) \end{bmatrix}, \; P(z) = \begin{bmatrix} P_1(z) & & 0 \\ & \ddots & \\ 0 & & P_N(z) \end{bmatrix}$$

If $\det(I - DK) \neq 0$*:*

$$(\mathcal{A}, \mathcal{B}) \text{ reachable} \;\Leftrightarrow\; (Q(z) - KP(z), L) \text{ left coprime}$$
$$(\mathcal{A}, \mathcal{C}) \text{ observable} \;\Leftrightarrow\; (Q(z) - KP(z), MP(z)) \text{ right coprime.}$$

Networks of Linear Systems

Theorem

(A_i, B_i, C_i, D_i) *reachable and observable for* $i = 1, \ldots, N$

Coprime factorization: $C_i(zI - A_i)^{-1}B_i + D_i = P_i(z)Q_i(z)^{-1}$

$$Q(z) = \begin{bmatrix} Q_1(z) & & 0 \\ & \ddots & \\ 0 & & Q_N(z) \end{bmatrix}, \; P(z) = \begin{bmatrix} P_1(z) & & 0 \\ & \ddots & \\ 0 & & P_N(z) \end{bmatrix}$$

If $\det(I - DK) \neq 0$*:*

$$(\mathcal{A}, \mathcal{B}) \text{ reachable } \Leftrightarrow \; (Q(z) - KP(z), L) \text{ left coprime}$$
$$(\mathcal{A}, \mathcal{C}) \text{ observable } \Leftrightarrow \; (Q(z) - KP(z), MP(z)) \text{ right coprime.}$$

Remark: Reachability/Observability of the single systems is necessary for reachability/observability of the network.

Reachability of General Networks

Theorem

Let K, L be arbitrary but fixed matrices. The probability that $(\mathcal{A}, \mathcal{B})$ is reachable if (A_i, B_i, C_i, D_i) are chosen randomly for $i = 1, \ldots, N$, is either equal to zero or $1 + O(t)$ for $t \to 0$.

Idea of proof: Schwartz-Zippel-Lemma

Reachability of General Networks

Theorem

Let K, L be arbitrary but fixed matrices. The probability that $(\mathcal{A}, \mathcal{B})$ is reachable if (A_i, B_i, C_i, D_i) are chosen randomly for $i = 1, \ldots, N$, is either equal to zero or $1 + O(t)$ for $t \to 0$.

Idea of proof: Schwartz-Zippel-Lemma

Definition

View the N node systems of a network as vertices of a graph and add a $N + 1$-th vertex, called input node.
Denote by Γ_{KL} the directed graph where there is an edge from vertex j to vertex i if and only if $K_{ij} \in \mathbb{F}^{p_j \times m_i}$ is not the zero matrix there is an edge from the input node to vertex i if and only if $L_i \in \mathbb{F}^{m_i \times m}$ is not the zero matrix.
A vertex of Γ_{KL} is called accessible if the graph contains a path from the input node to this vertex.

Reachability of General Networks

Theorem

(i) If Γ_{KL} contains a nonaccessible vertex, $(\mathcal{A}, \mathcal{B})$ is not reachable, i.e. the probability of reachability is zero.
(ii) If all vertices of Γ_{KL} are accessible, there exists $s \in \mathbb{N}$ such that $(\mathcal{A}, \mathcal{B})$ is reachable over the extension field $\mathbb{F}^r$ of $\mathbb{F}$ with probability $1 + O(t^r)$ if $r \geq s$ and with probability zero if $r < s$.

Idea of proof:
Transfering results about structural controlability over $\mathbb{R}$ to $\mathbb{F}$

- C. Lin: Structural controllability, IEEE Transactions on Automatic Control, Vol.19, No.3, 201-208, 1974.
- H. Mayeda: On structural controllability theorem, IEEE Transactions on Automatic Control, Vol.26, No.3, 795-798, 1981.

Reachability of Parallel Connections

$$\begin{aligned} x_1(\tau+1) &= A_1 x_1(\tau) + B_1 u(\tau) \\ &\vdots \\ x_N(\tau+1) &= A_N x_N(\tau) + B_N u(\tau) \end{aligned} \tag{2}$$

$(C_i, D_i) = (I_n, 0)$, $K = 0$, $L^\top = [I_m \dots I_m]$ and $I - DK$ invertible

Reachability of Parallel Connections

$$\begin{aligned} x_1(\tau+1) &= A_1 x_1(\tau) + B_1 u(\tau) \\ &\vdots \\ x_N(\tau+1) &= A_N x_N(\tau) + B_N u(\tau) \end{aligned} \tag{2}$$

$(C_i, D_i) = (I_n, 0)$, $K = 0$, $L^\top = [I_m \dots I_m]$ and $I - DK$ invertible

$$[Q - KP\ L] = \begin{bmatrix} Q_1(z) & & & I_m \\ & \ddots & & \vdots \\ & & Q_N(z) & I_m \end{bmatrix} \text{ left prime}$$

$$\Leftrightarrow \begin{bmatrix} Q_1(z) & -Q_2(z) & & \\ & \ddots & \ddots & \\ & & Q_{N-1}(z) & -Q_N(z) \end{bmatrix} \text{ left prime}$$

Reachability of Parallel Connections

Proposition (FH 2015)

System (2) *reachable if and only if*
(a) (A_i, B_i) *reachable for* $i = 1, \ldots, N$
(b) $Q_1(z), .., Q_N(z)$ *mutually left coprime, i.e.* $Q_i(z)$ *left coprime with the least common right multiple of all* $Q_j(z)$ *with* $j \neq i$

Reachability of Parallel Connections

Proposition (FH 2015)

System (2) *reachable if and only if*
(a) (A_i, B_i) *reachable for* $i = 1, \ldots, N$
(b) $Q_1(z), .., Q_N(z)$ *mutually left coprime, i.e.* $Q_i(z)$ *left coprime with the least common right multiple of all* $Q_j(z)$ *with* $j \neq i$

Theorem

The probability that the parallel connection (2) *is reachable is*

$$\left(1 - \sum_{k=2}^{m+1} \binom{N}{k} t^m + O\left(t^{m+1}\right)\right) \prod_{i=1}^{N} \prod_{j=m}^{n_i+m-1} \left(1 - t^j\right) =$$

$$= 1 - \sum_{k=1}^{m+1} \binom{N}{k} t^m + O\left(t^{m+1}\right).$$

Reachability of Parallel Connections

Idea of proof (Probability of mutual coprimeness)

- Restriction to generic class of polynomial matrices in Hermite form
- Recursion formula for probability that N polynomial matrices in Hermite form are mutually coprime

Remark:
Mutual coprimeness is **stronger** than coprimeness or pairwise coprimeness!

Parallel Connection: Single-Input

Theorem

The probability that the parallel connection of N single-input systems is reachable is equal to

$$1 - \frac{N(N+1)}{2}t + C_2(N)t^2 + O(t^3)$$

where N_1 *is the number of systems with scalar state vector and*

$$C_2(N) = \frac{1}{24}(N-1)(N-2)(3N^2 + 11N - 12N_1) + \frac{N^3 - 3N}{2}.$$

Parallel Connection: Single-Input

Theorem

The probability that the parallel connection of N single-input systems is reachable is equal to

$$1 - \frac{N(N+1)}{2}t + C_2(N)t^2 + O(t^3)$$

where N_1 is the number of systems with scalar state vector and

$$C_2(N) = \frac{1}{24}(N-1)(N-2)(3N^2 + 11N - 12N_1) + \frac{N^3 - 3N}{2}.$$

Idea of proof:

- Inclusion-exclusion principle
- Estimation per induction

Reachability of Series Connections

$$K = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ I_{p_1} & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ 0 & & I_{p_{N-1}} & 0 \end{bmatrix}, \; L = \begin{bmatrix} I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; \det(I - DK) = 1 \neq 0$$

Reachability of Series Connections

$$K = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ I_{p_1} & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ 0 & & I_{p_{N-1}} & 0 \end{bmatrix}, \; L = \begin{bmatrix} I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; \det(I - DK) = 1 \neq 0$$

$$\begin{bmatrix} Q_1(z) & & & & I_m \\ -P_1(z) & Q_2(z) & & & 0 \\ & \ddots & \ddots & & \vdots \\ & & -P_{N-1}(z) & Q_N(z) & 0 \end{bmatrix} \text{ left prime}$$

$$\Leftrightarrow \begin{bmatrix} -P_1(z) & Q_2(z) & & \\ & \ddots & \ddots & \\ & & -P_{N-1}(z) & Q_N(z) \end{bmatrix} \text{ left prime}$$

Series Connection: Single-input Single-output

Theorem

The probability that the series connection of N reachable and observable single-input single-output systems is reachable is

$$1 - \binom{N}{2} t + O(t^2).$$

Theorem

The probability that the series connection of N reachable and observable single-input single-output systems with strictly proper transfer functions is reachable is equal to

$$1 - \sum_{1 \le i < N,\ n_i \neq 1} (N - i) \cdot t + O(t^2) =$$

$$= 1 - \left(\frac{N(N-1)}{2} - \sum_{1 \le i < N,\ n_i = 1} (N - i) \right) \cdot t + O(t^2).$$

Series Connection of two Systems

$$\begin{aligned} x_1(\tau+1) &= A_1 x_1(\tau) + B_1 u(\tau) \\ x_2(\tau+1) &= A_2 x_2(\tau) + B_2 C_1 x_1(\tau) + B_2 D_1 u(\tau) \end{aligned} \tag{3}$$

$A_i \in \mathbb{F}^{n_i \times n_i}, B_1 \in \mathbb{F}^{n_1 \times m}, B_2 \in \mathbb{F}^{n_2 \times p_1}, C_i \in \mathbb{F}^{p_i \times n_i}, D_i \in \mathbb{F}^{p_i \times m}$

Series Connection of two Systems

$$\begin{aligned} x_1(\tau+1) &= A_1 x_1(\tau) + B_1 u(\tau) \\ x_2(\tau+1) &= A_2 x_2(\tau) + B_2 C_1 x_1(\tau) + B_2 D_1 u(\tau) \end{aligned} \tag{3}$$

$A_i \in \mathbb{F}^{n_i \times n_i}$, $B_1 \in \mathbb{F}^{n_1 \times m}$, $B_2 \in \mathbb{F}^{n_2 \times p_1}$, $C_i \in \mathbb{F}^{p_i \times n_i}$, $D_i \in \mathbb{F}^{p_i \times m}$

Proposition (FH 2015)

For $i = 1, 2$, let (A_i, B_i, C_i, D_i) be reachable and observable. Then, system (3) is reachable if and only if $P_1 \in \mathbb{F}[z]^{p_1 \times m}$ and $Q_2 \in \mathbb{F}[z]^{p_1 \times p_1}$ are left coprime.

Series Connection of two Systems

$$\begin{aligned} x_1(\tau+1) &= A_1 x_1(\tau) + B_1 u(\tau) \\ x_2(\tau+1) &= A_2 x_2(\tau) + B_2 C_1 x_1(\tau) + B_2 D_1 u(\tau) \end{aligned} \tag{3}$$

$A_i \in \mathbb{F}^{n_i \times n_i}, B_1 \in \mathbb{F}^{n_1 \times m}, B_2 \in \mathbb{F}^{n_2 \times p_1}, C_i \in \mathbb{F}^{p_i \times n_i}, D_i \in \mathbb{F}^{p_i \times m}$

Proposition (FH 2015)

For $i = 1, 2$, let (A_i, B_i, C_i, D_i) be reachable and observable. Then, system (3) is reachable if and only if $P_1 \in \mathbb{F}[z]^{p_1 \times m}$ and $Q_2 \in \mathbb{F}[z]^{p_1 \times p_1}$ are left coprime.

Theorem

The probability that the series connection of two reachable and observable systems (A_i, B_i, C_i, D_i) for $i = 1, 2$ is reachable is

$$1 - t^m + O\left(t^{m+1}\right).$$

Series Connections of two Strictly Proper Systems

Theorem

The probability that the series connection of two reachable and observable systems with strictly proper transfer functions is reachable is equal to

$$
\begin{aligned}
1 \quad & \text{for } p_1 = n_1 = 1, \\
1 - t^{m_1} + O(t^{m_1+1}) \quad & \text{for } p_1 = 1,\ n_1 > 1 \text{ or } p_1 \geq 2,\ n_1 > m_1 \\
& \text{or } p_1 \geq 2,\ m_1 = 1, \\
1 - 2t^{m_1} + O(t^{m_1+1}) \quad & \text{for } p_1 \geq 2,\ n_1 = m_1 \neq 1, \\
1 - t^{n_1} + O(t^{n_1+1}) \quad & \text{for } p_1 \geq 2,\ n_1 < m_1 .
\end{aligned}
$$

Reachability of Circular Interconnections

$$K = \begin{bmatrix} 0 & \cdots & 0 & I_{p_N} \\ I_{p_1} & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & I_{p_{N-1}} & 0 \end{bmatrix}, L = \begin{bmatrix} I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Remark:

- Same coprimeness conditions as for series connection
- Additional condition $\det(I - DK) = \det(I - D_N \cdots D_1) \neq 0$
- Same asymptotic formulas for probability of reachability as for series connection in all considered cases, i.e. for N SISO systems and two arbitrary systems (feedback interconnection), proper and strictly proper, respectively

Convolutional Codes

Definition

A **convolutional code** $\mathfrak{C}$ of **rate** k/n is a free $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$ of rank k.
There exists $G \in \mathbb{F}[z]^{n \times k}$ of full column rank such that

$$\mathfrak{C} = \{v \in \mathbb{F}[z]^n \mid v(z) = G(z)m(z) \text{ for some } m \in \mathbb{F}[z]^k\}.$$

G is called **generator matrix** of the code and is unique up to right multiplication with a unimodular matrix $U \in Gl_k(\mathbb{F}[z])$.

Convolutional Codes

Definition

Let $\nu_1, \ldots, \nu_k$ be the column degrees of G. Then, $\nu := \nu_1 + \cdots + \nu_k$ is called the **order** of G. The **degree** δ of $\mathfrak{C}$ is defined as the minimal order of its generator matrices.

Convolutional Codes

Definition

Let $\nu_1, \ldots, \nu_k$ be the column degrees of G. Then, $\nu := \nu_1 + \cdots + \nu_k$ is called the **order** of G. The **degree** δ of $\mathfrak{C}$ is defined as the minimal order of its generator matrices.

Lemma

It holds $\nu = \delta$, i.e. G is a minimal basis of $\mathfrak{C}$, if and only if G is column proper.

Convolutional Codes

Definition

Let $\nu_1, \ldots, \nu_k$ be the column degrees of G. Then, $\nu := \nu_1 + \cdots + \nu_k$ is called the **order** of G. The **degree** δ of $\mathfrak{C}$ is defined as the minimal order of its generator matrices.

Lemma

It holds $\nu = \delta$, i.e. G is a minimal basis of $\mathfrak{C}$, if and only if G is column proper.

Definition

A convolutional code $\mathfrak{C}$ is called **non-catastrophic** if one and therefore, each of its generator matrices is right prime.

Convolutional Codes and Linear Systems

Let $(A, B, C, D) \in \mathbb{F}^{s\times s} \times \mathbb{F}^{s\times k} \times \mathbb{F}^{n-k\times s} \times \mathbb{F}^{n-k\times k}$ and $H(z) := \begin{bmatrix} zI - A & 0_{s\times(n-k)} & -B \\ -C & I_{n-k} & -D \end{bmatrix}$.

The set of $\begin{pmatrix} y \\ u \end{pmatrix} \in \mathbb{F}[z]^n$ with $y \in \mathbb{F}[z]^{n-k}$ and $u \in \mathbb{F}[z]^k$ for which there exists $x \in \mathbb{F}[z]^s$ with $H(z) \cdot [x(z)\ y(z)\ u(z)]^\top = 0$ forms a submodule of $\mathbb{F}[z]^n$ of rank k and thus, a convolutional code of rate k/n, which is denoted by $\mathfrak{C}(A, B, C, D)$.

Convolutional Codes and Linear Systems

Let $(A, B, C, D) \in \mathbb{F}^{s\times s} \times \mathbb{F}^{s\times k} \times \mathbb{F}^{n-k\times s} \times \mathbb{F}^{n-k\times k}$ and $H(z) := \begin{bmatrix} zI - A & 0_{s\times(n-k)} & -B \\ -C & I_{n-k} & -D \end{bmatrix}$.

The set of $\begin{pmatrix} y \\ u \end{pmatrix} \in \mathbb{F}[z]^n$ with $y \in \mathbb{F}[z]^{n-k}$ and $u \in \mathbb{F}[z]^k$ for which there exists $x \in \mathbb{F}[z]^s$ with $H(z) \cdot [x(z)\ y(z)\ u(z)]^\top = 0$ forms a submodule of $\mathbb{F}[z]^n$ of rank k and thus, a convolutional code of rate k/n, which is denoted by $\mathfrak{C}(A, B, C, D)$.
Moreover, there exist $X \in \mathbb{F}[z]^{s\times k}$, $Y \in \mathbb{F}[z]^{(n-k)\times k}$, $U \in \mathbb{F}[z]^{k\times k}$ such that $\ker(H(z)) = \mathrm{im}[X(z)\ Y(z)\ U(z)]^\top$ and $G = \begin{pmatrix} Y \\ U \end{pmatrix}$ is a generator matrix for $\mathfrak{C}$ with $C(zI - A)^{-1}B + D = Y(z)U(z)^{-1}$.

Convolutional Codes and Linear Systems

Conversely, for each convolutional code $\mathfrak{C}$ of rate k/n and degree δ, there is $(A, B, C, D) \in \mathbb{F}^{s\times s} \times \mathbb{F}^{s\times k} \times \mathbb{F}^{n-k\times s} \times \mathbb{F}^{n-k\times k}$ with $s \geq \delta$ such that $\mathfrak{C} = \mathfrak{C}(A, B, C, D)$.
Moreover, it is always possible to choose $s = \delta$. In this case, one calls (A, B, C, D) a **minimal representation** of $\mathfrak{C}$.

Convolutional Codes and Linear Systems

Conversely, for each convolutional code $\mathfrak{C}$ of rate k/n and degree δ, there is $(A, B, C, D) \in \mathbb{F}^{s\times s} \times \mathbb{F}^{s\times k} \times \mathbb{F}^{n-k\times s} \times \mathbb{F}^{n-k\times k}$ with $s \geq \delta$ such that $\mathfrak{C} = \mathfrak{C}(A, B, C, D)$.
Moreover, it is always possible to choose $s = \delta$. In this case, one calls (A, B, C, D) a **minimal representation** of $\mathfrak{C}$.

Theorem (RY 1999)

(A, B, C, D) is a minimal representation of $\mathfrak{C}(A, B, C, D)$ if and only if it is reachable.

Convolutional Codes and Linear Systems

Conversely, for each convolutional code $\mathfrak{C}$ of rate k/n and degree δ, there is $(A, B, C, D) \in \mathbb{F}^{s\times s} \times \mathbb{F}^{s\times k} \times \mathbb{F}^{n-k\times s} \times \mathbb{F}^{n-k\times k}$ with $s \geq \delta$ such that $\mathfrak{C} = \mathfrak{C}(A, B, C, D)$.
Moreover, it is always possible to choose $s = \delta$. In this case, one calls (A, B, C, D) a **minimal representation** of $\mathfrak{C}$.

Theorem (RY 1999)

(A, B, C, D) is a minimal representation of $\mathfrak{C}(A, B, C, D)$ if and only if it is reachable.

Theorem (RY 1999)

Assume that (A, B, C, D) is reachable. Then $\mathfrak{C}(A, B, C, D)$ is non-catastrophic if and only if (A, B, C, D) is observable.

RY 1999: J. Rosenthal, E.V. York: BCH convolutional codes, IEEE Trans. Inform. Theory, Vol. 45, No. 6 (1999), 1833-1844.

Convolutional Codes and Linear Systems

Theorem

The probability that a convolutional code $\mathfrak{C}(A, B, C, D)$ *of rate* k/n *and degree* δ *is non-catastrophic is equal to*

$$P^{rc}_{n-k,\delta,k} = \frac{\Pr((A, B, C, D) \textit{ reachable and observable})}{\Pr((A, B, C, D) \textit{ reachable})} = \\ = 1 - t^{n-k} + O(t^{n-k+1}).$$

Convolutional Codes and Linear Systems

Theorem

The probability that a convolutional code $\mathfrak{C}(A, B, C, D)$ of rate k/n and degree δ is non-catastrophic is equal to

$$P^{rc}_{n-k,\delta,k} = \frac{\Pr((A, B, C, D) \textit{ reachable and observable})}{\Pr((A, B, C, D) \textit{ reachable})} = \\ = 1 - t^{n-k} + O(t^{n-k+1}).$$

There are two possibilities to prove this theorem:

(1) Probability that $G = \begin{pmatrix} Y \\ U \end{pmatrix}$ with YU^{-1} proper is right prime is equal to $P^{rc}_{n-k,\delta,k}$ (remaining equations are already known).
(2): Using the correspondence between non-catastrophicity of convolutional codes and observability of linear systems

Interconnected Convolutional Codes

Theorem

For $i = 1, \ldots, N$, let $\mathfrak{C}_i = \mathfrak{C}(A_i, B_i, C_i, D_i)$ be non-catastrophic with (A_i, B_i, C_i, D_i) reachable and observable.
With the same notation as for networks of linear systems, set

$$\mathcal{A} = A + BK(I - DK)^{-1}C, \qquad \mathcal{B} = B(I - KD)^{-1}L$$
$$\mathcal{C} = M(I - DK)^{-1}C, \qquad \mathcal{D} = M(I - DK)^{-1}DL + J.$$

Coprime factorization: $C_i(zI - A_i)^{-1}B_i + D_i = P_i(z)Q_i(z)^{-1}$
If $\det(I - DK) \neq 0$*:*

$(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *minimal representation of* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$
$\Leftrightarrow$ $(Q(z) - KP(z), L)$ *left coprime*
$(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *minimal representation of non-catastrophic* $\mathfrak{C}$
$\Leftrightarrow$ $(Q(z) - KP(z), L)$ *l.c. and* $(Q(z) - KP(z), MP(z))$ *r.c.*

Series Connection of two Convolutional Codes

$$K = \begin{bmatrix} 0 & 0 \\ I_{k_2} & 0 \end{bmatrix}, L = \begin{bmatrix} I_{k_1} \\ 0 \end{bmatrix}, M = I_{n_2}, \det(I - DK) = 1 \neq 0$$

In CHP 2007, sufficient criteria for $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ to be a minimal representation of $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ were provided.

$$[Q(z) - KP(z)\ L] \text{ left prime} \Leftrightarrow\ [P_1\ Q_2] \text{ left prime}$$

Theorem

Let $(A_i, B_i, C_i, D_i) \in \mathbb{F}^{\delta_i \times \delta_i} \times \mathbb{F}^{\delta_i \times k_i} \times \mathbb{F}^{(n_i - k_i) \times \delta_i} \times \mathbb{F}^{(n_i - k_i) \times k_i}$ *be minimal representations of the non-catastrophic convolutional codes* $\mathfrak{C}(A_i, B_i, C_i, D_i)$ *for* $i = 1, 2$*. Then, the probability that* $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is a minimal representation for the series connected code* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *(and that* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is non-catastrophic) is*

$$1 - t^{k_1} + O\left(t^{k_1+1}\right).$$

CHP 2007: Climent, J.-J. et al.: A first approximation of concatenated convolutional codes from linear systems theory viewpoint, Lin. Alg. Appl., 425(2007), 673-699.

Series Connection of two Convolutional Codes

Furthermore, the probability that this interconnection is minimal is equal to the probability that the single systems are minimal and P_1 and Q_2 are left coprime. Hence, one has:

Theorem

Let $(A_i, B_i, C_i, D_i) \in \mathbb{F}^{\delta_i \times \delta_i} \times \mathbb{F}^{\delta_i \times k_i} \times \mathbb{F}^{(n_i - k_i) \times \delta_i} \times \mathbb{F}^{(n_i - k_i) \times k_i}$ *be randomly for* $i = 1, 2$. *Then, the probability that* $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is a minimal representation for the series connected code* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *and that* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is non-catastrophic is*

$$\prod_{i=1}^{2} (1 - t^{k_i} - t^{n_i - k_i} + O(t^{\min(k_i, n_i - k_i) + 1})) \cdot (1 - t^{k_1} + O(t^{k_1 + 1})) =$$

$$= 1 - 2t^{k_1} - 2t^{k_2} - t^{n_2 - k_2} + O(t^{\min(k_1, k_2, n_2 - k_2) + 1})$$

since $n_1 - k_1 = k_2$.

Turbo codes: Interleaved Parallel Connection

$$K = 0,\ L = \begin{bmatrix} \pi_1 \\ \vdots \\ \pi_N \end{bmatrix},\ M = I,\ \pi_i \in S_k,\ \det(I - DK) = 1$$

$[Q(z) - KP(z)\ L]$ l.p. $\Leftrightarrow$ $\pi_1^{-1} Q_1, \ldots \pi_N^{-1} Q_N$ mutually left coprime

Turbo codes: Interleaved Parallel Connection

$$K = 0,\ L = \begin{bmatrix} \pi_1 \\ \vdots \\ \pi_N \end{bmatrix},\ M = I,\ \pi_i \in S_k,\ \det(I - DK) = 1$$

$[Q(z) - KP(z)\ L]$ l.p. $\Leftrightarrow$ $\pi_1^{-1} Q_1, \ldots \pi_N^{-1} Q_N$ mutually left coprime

Theorem

Let $(A_i, B_i, C_i, D_i) \in \mathbb{F}^{\delta_i \times \delta_i} \times \mathbb{F}^{\delta_i \times k} \times \mathbb{F}^{(n_i - k) \times \delta_i} \times \mathbb{F}^{(n_i - k) \times k}$ *be minimal representations of the non-catastrophic convolutional codes* $\mathfrak{C}(A_i, B_i, C_i, D_i)$ *for* $i = 1, 2$*. Then, the probability that* $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is a minimal representation for the turbo code* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *(and that* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is non-catastrophic) is*

$$1 - \sum_{y=2}^{k+1} \binom{N}{y} t^k + O(t^{k+1}).$$

Turbo codes: Interleaved Parallel Connection

Furthermore, the probability that this interconnection is minimal is equal to the probability that the single systems are minimal and $\pi_1^{-1}Q_1, \ldots \pi_N^{-1}Q_N$ are mutually left coprime. Hence, one has:

Theorem

Let $(A_i, B_i, C_i, D_i) \in \mathbb{F}^{\delta_i \times \delta_i} \times \mathbb{F}^{\delta_i \times k} \times \mathbb{F}^{(n_i-k)\times \delta_i} \times \mathbb{F}^{(n_i-k)\times k}$ *be randomly for* $i = 1, \ldots, N$. *Then, the probability that* $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is a minimal representation for the turbo code* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *and that* $\mathfrak{C}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ *is non-catastrophic is*

$$\left(1 - \sum_{y=2}^{k+1} \binom{N}{y} t^k + O(t^{k+1})\right) \prod_{i=1}^{N} (1 - t^k - t^{n_i-k} + O(t^{\min(k, n_i-k)})).$$