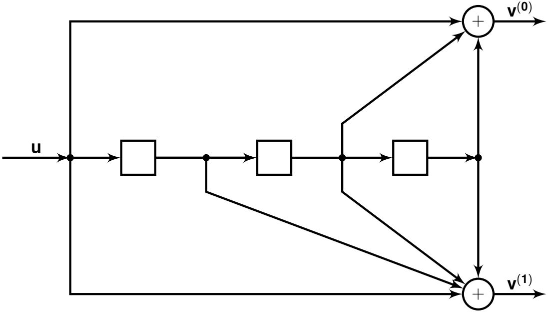
Convolutional Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

October 23, 2015

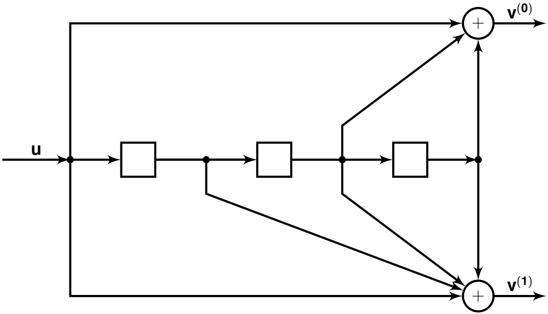
Example 1



- Message bits $\mathbf{u} = (u_0, u_1, u_2, \ldots)$
- Outputs $\mathbf{v}^{(0)} = (v_0^{(0)}, v_1^{(0)}, v_2^{(0)}, \ldots)$, $\mathbf{v}^{(1)} = (v_0^{(1)}, v_1^{(1)}, \ldots)$

$$
\begin{aligned}
v_i^{(0)} &= u_i + u_{i-2} + u_{i-3} \\
v_i^{(1)} &= u_i + u_{i-1} + u_{i-2} + u_{i-3}
\end{aligned}
$$

Example 1

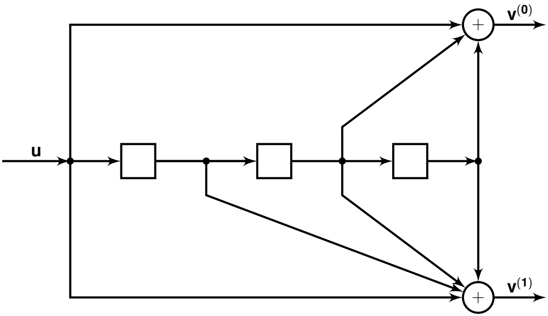


- Outputs are multiplexed into a single sequence

$$\mathbf{v} = \begin{bmatrix} v_0^{(0)} & v_0^{(1)} & v_1^{(0)} & v_1^{(1)} & v_2^{(0)} & v_2^{(1)} & \cdots \end{bmatrix}$$

- Rate of the code is $\frac{1}{2}$
- Encoder has memory order 3

Example 1



- Impulse responses of the encoder

$$\mathbf{g}^{(0)} = \begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$$
$$\mathbf{g}^{(1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Example 1

- Impulse responses of the encoder

$$\begin{aligned}\mathbf{g}^{(0)} &= \begin{bmatrix}1 & 0 & 1 & 1\end{bmatrix}\\ \mathbf{g}^{(1)} &= \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}\end{aligned}$$

- Outputs in terms of impulse responses

$$\begin{aligned}v_i^{(0)} &= u_i + u_{i-2} + u_{i-3} = \sum_{j=0}^{3} u_{i-j} g_j^{(0)}\\ v_i^{(1)} &= u_i + u_{i-1} + u_{i-2} + u_{i-3} = \sum_{j=0}^{3} u_{i-j} g_j^{(1)}\end{aligned}$$

$$\begin{aligned}\mathbf{v}^{(0)} &= \mathbf{u} \odot \mathbf{g}^{(0)}\\ \mathbf{v}^{(1)} &= \mathbf{u} \odot \mathbf{g}^{(1)}\end{aligned}$$

Example 1

$$\begin{aligned} v_i^{(0)} &= u_i + u_{i-2} + u_{i-3} \\ v_i^{(1)} &= u_i + u_{i-1} + u_{i-2} + u_{i-3} \end{aligned}$$

- If **u** has length 5, then the output **v** has length 16
- If $\mathbf{v} = \mathbf{u}\mathbf{G}$ where **G** is a 5×16 matrix, then

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & & & & & & \\ & & & & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & & & & \\ & & & & & & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & & \\ & & & & & & & & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Example 1

- Transform domain representation of the generator matrix is

$$\mathbf{G}(D) = \left[\mathbf{g}^{(0)}(D) \quad \mathbf{g}^{(1)}(D)\right] = \left[1 + D^2 + D^3 \quad 1 + D + D^2 + D^3\right]$$

- For input polynomial $\mathbf{u}(D)$ given by

$$\mathbf{u}(D) = u_0 + u_1 D + u_2 D^2 + \cdots$$

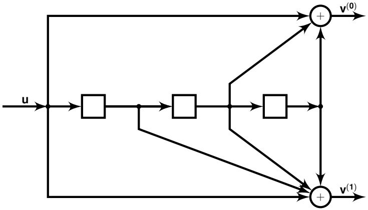
the output polynomials are given by

$$\begin{aligned} \mathbf{v}^{(0)}(D) = v_0^{(0)} + v_1^{(0)} D + v_2^{(0)} D^2 + \cdots &= \mathbf{u}(D)\mathbf{g}^{(0)}(D) \\ \mathbf{v}^{(1)}(D) = v_0^{(1)} + v_1^{(1)} D + v_2^{(1)} D^2 + \cdots &= \mathbf{u}(D)\mathbf{g}^{(1)}(D) \end{aligned}$$

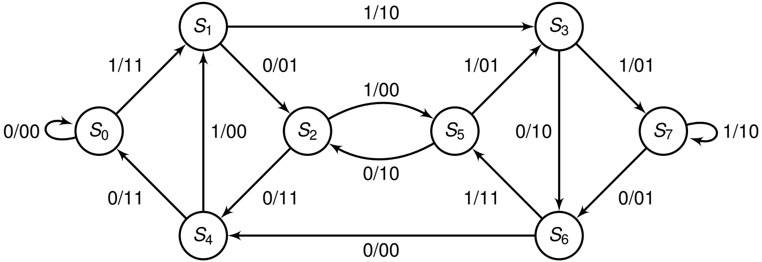
- After multiplexing the output polynomial is

$$\mathbf{v}(D) = \mathbf{v}^{(0)}(D^2) + D\mathbf{v}^{(1)}(D^2)$$

Example 1



Encoder state diagram



Example 1

- The set of outputs $\mathbf{v}(D) = \mathbf{u}(D)\mathbf{G}(D)$ are the codewords corresponding to

$$\mathbf{G}(D) = \begin{bmatrix} 1 + D^2 + D^3 & 1 + D + D^2 + D^3 \end{bmatrix}$$

- The following systematic generator matrix also generates the same codewords

$$\mathbf{G}'(D) = \begin{bmatrix} 1 & \frac{1+D+D^2+D^3}{1+D^2+D^3} \end{bmatrix}$$

- If $\mathbf{v}(D) = \mathbf{u}(D)\mathbf{G}(D)$ then

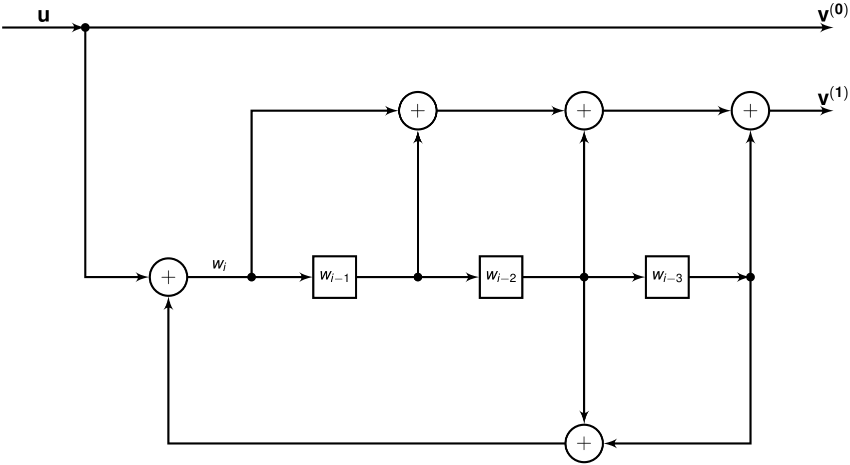
$$\mathbf{v}(D) = \mathbf{u}(D)(1 + D^2 + D^3)\mathbf{G}'(D)$$

- If $\mathbf{v}(D) = \mathbf{u}(D)\mathbf{G}'(D)$ then

$$\mathbf{v}(D) = \frac{\mathbf{u}(D)}{(1 + D^2 + D^3)}\mathbf{G}(D)$$

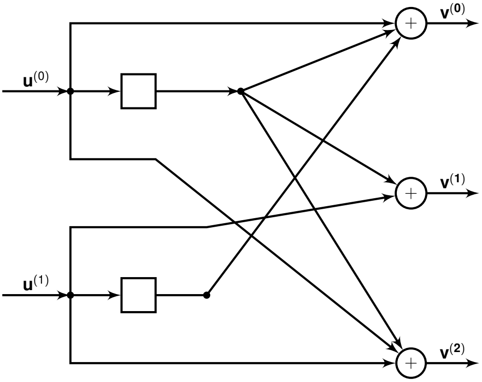
Example 1

Encoder circuit corresponding to $\mathbf{G}'(D) = \begin{bmatrix} 1 & \frac{1+D+D^2+D^3}{1+D^2+D^3} \end{bmatrix}$



This is a systematic feedback encoder

Example 2



$$
\begin{aligned}
v_i^{(0)} &= u_i^{(0)} + u_{i-1}^{(0)} + u_{i-1}^{(1)} \\
v_i^{(1)} &= u_{i-1}^{(0)} + u_i^{(1)} \\
v_i^{(2)} &= u_i^{(0)} + u_{i-1}^{(0)} + u_i^{(1)}
\end{aligned}
$$

Example 2

- Impulse responses of the encoder

$$\mathbf{g}_0^{(0)} = \begin{bmatrix}1 & 1\end{bmatrix}, \quad \mathbf{g}_0^{(1)} = \begin{bmatrix}0 & 1\end{bmatrix}, \quad \mathbf{g}_0^{(2)} = \begin{bmatrix}1 & 1\end{bmatrix}$$

$$\mathbf{g}_1^{(0)} = \begin{bmatrix}0 & 1\end{bmatrix}, \quad \mathbf{g}_1^{(1)} = \begin{bmatrix}1 & 0\end{bmatrix}, \quad \mathbf{g}_1^{(2)} = \begin{bmatrix}1 & 0\end{bmatrix}$$

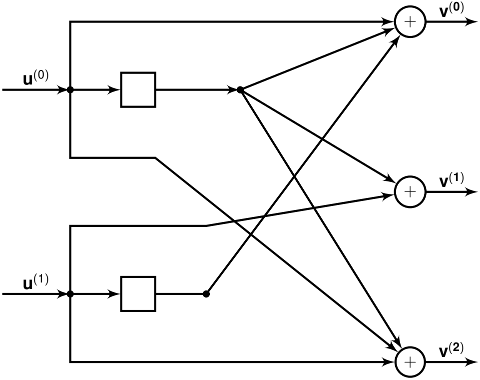
- Outputs in terms of impulse responses

$$\begin{aligned}
\mathbf{v}^{(0)} &= \mathbf{u}^{(0)} \odot \mathbf{g}_0^{(0)} + \mathbf{u}^{(1)} \odot \mathbf{g}_1^{(0)} \\
\mathbf{v}^{(1)} &= \mathbf{u}^{(0)} \odot \mathbf{g}_0^{(1)} + \mathbf{u}^{(1)} \odot \mathbf{g}_1^{(1)} \\
\mathbf{v}^{(2)} &= \mathbf{u}^{(0)} \odot \mathbf{g}_0^{(2)} + \mathbf{u}^{(1)} \odot \mathbf{g}_1^{(2)}
\end{aligned}$$

- Transform domain representation of the generator matrix is

$$\mathbf{G}(D) = \begin{bmatrix} \mathbf{g}_0^{(0)}(D) & \mathbf{g}_0^{(1)}(D) & \mathbf{g}_0^{(2)}(D) \\ \mathbf{g}_1^{(0)}(D) & \mathbf{g}_1^{(1)}(D) & \mathbf{g}_1^{(2)}(D) \end{bmatrix} = \begin{bmatrix} 1+D & D & 1+D \\ D & 1 & 1 \end{bmatrix}$$

Example 2



- Rate of the code is $\frac{2}{3}$
- Encoder has memory order 1
- Overall constraint length is 2

Defining a Convolutional Encoder

- Maps k inputs to n outputs
- Linearly maps input sequences of arbitrary length to output sequences
  - What are the domain and range of the encoder?
- Has a transform domain generator matrix with rational function entries
  - Can any arbitrary rational function appear in the generator matrix?

Binary Laurent Series

- Let $\mathbb{F}_2((D))$ be the set of expressions $x(D) = \sum_{i=m}^{\infty} x_i D^i$ where $m \in \mathbb{Z}$ and $x_i \in \mathbb{F}_2$
- $x(D) \in \mathbb{F}_2((D))$ has finitely many negative powers of D
- For $y(D) = \sum_{i=n}^{\infty} y_i D^i$, define the operations of addition and multiplication on $\mathbb{F}_2((D))$ as

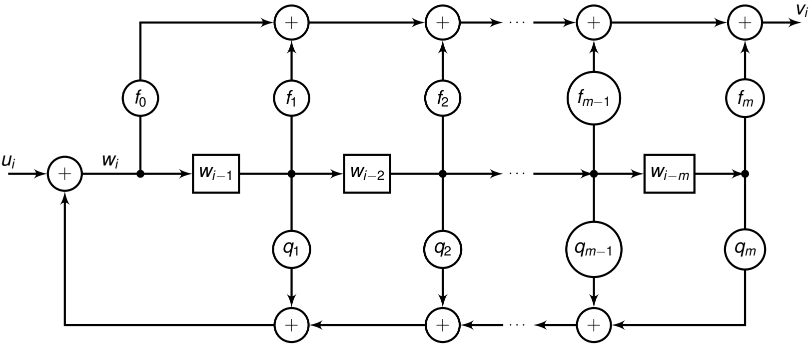
$$
\begin{aligned}
x(D) + y(D) &= \sum_{\min(m,n)}^{\infty} (x_i + y_i) D^i \\
x(D) * y(D) &= \sum_{k=m+n}^{\infty} \left(\sum_{i+j=k} x_i y_j \right) D^k
\end{aligned}
$$

- $\mathbb{F}_2((D))$ is a field
- A convolutional encoder is a linear map from $\mathbb{F}_2^k((D))$ to $\mathbb{F}_2^n((D))$

Realizable Rational Functions

- A rational transfer function $g(D) = f(D)/q(D)$ is said to be realizable if $q(0) = 1$
- Let $v(D) = u(D)g(D)$ where

$$g(D) = \frac{f_0 + f_1 D + \cdots + f_m D^m}{1 + q_1 D + \cdots + q_m D^m}$$



Convolutional Codes

- Let $\mathbb{F}_2(D)$ be the set of rational functions with coefficients in $\mathbb{F}_2$
- A convolutional encoder is a linear mapping from $\mathbb{F}_2^k((D))$ to $\mathbb{F}_2^n((D))$ which can be represented as

$$\mathbf{v}(D) = \mathbf{u}(D)\mathbf{G}(D)$$

  where $\mathbf{u}(D) \in \mathbb{F}_2^k((D))$, $\mathbf{v}(D) \in \mathbb{F}_2^n((D))$ and $\mathbf{G}(D)$ is $k \times n$ transfer function matrix having rank k with entries in $\mathbb{F}_2(D)$ each of which is realizable
- A rate $\frac{k}{n}$ convolutional code is the image set of a convolutional encoder with a $k \times n$ transfer function matrix
- $\mathbf{G}(D)$ is called a generator matrix of the code

Equivalent Generator Matrices

- Two convolutional generator matrices $\mathbf{G}(D)$ and $\mathbf{G}'(D)$ are equivalent if they generate the same code
- $\mathbf{G}(D)$ and $\mathbf{G}'(D)$ are equivalent $\iff$ there is a nonsingular matrix $\mathbf{T}(D)$ over $\mathbb{F}_2(D)$ such that

$$\mathbf{G}(D) = \mathbf{T}(D)\mathbf{G}'(D)$$

- Example 1

$$\begin{aligned}\mathbf{G}(D) &= \begin{bmatrix} 1+D^2+D^3 & 1+D+D^2+D^3 \end{bmatrix} \\ \mathbf{G}'(D) &= \begin{bmatrix} 1 & \frac{1+D+D^2+D^3}{1+D^2+D^3} \end{bmatrix}\end{aligned}$$

- Example 2

$$\begin{aligned}\mathbf{G}(D) &= \begin{bmatrix} 1+D & D & 1+D \\ D & 1 & 1 \end{bmatrix} \\ \mathbf{G}'(D) &= \begin{bmatrix} 1 & 0 & 1/(1+D+D^2) \\ 0 & 1 & (1+D^2)/(1+D+D^2) \end{bmatrix}\end{aligned}$$

Catastrophic Generator Matrices

- Example

$$\begin{aligned}\mathbf{G}(D) &= \begin{bmatrix}1+D & 1+D^2\end{bmatrix} \\ \mathbf{u}(D) &= \frac{1}{1+D} = 1 + D + D^2 + D^3 + D^4 + \cdots \\ \mathbf{v}(D) &= \mathbf{u}(D)\mathbf{G}(D) = \begin{bmatrix}1 & 1+D\end{bmatrix}\end{aligned}$$

  - $\mathbf{v}(D)$ has weight 3 while $\mathbf{u}(D)$ has infinite weight
  - If the channel flips the 1s in $\mathbf{v}(D)$, the decoder will output $\hat{\mathbf{u}}(D) = 0$ causing an infinite number of decoding errors
- A generator matrix for a convolutional code is catastrophic if there exists an infinite weight input $\mathbf{u}(D)$ which results in a finite weight output $\mathbf{v}(D)$
- A convolutional encoder is catastrophic $\iff$ its state diagram has a zero-weight cycle other than the self-loop around the all-zeros state

Non-catastrophic Generator Matrices

- A systematic generator matrix is not catastrophic
- An $n \times k$ matrix $\widetilde{\mathbf{G}^{-1}}(D)$ over $\mathbb{F}_2(D)$ is called a right pseudo inverse of the $k \times n$ matrix $\mathbf{G}(D)$ if

$$\mathbf{G}(D)\widetilde{\mathbf{G}^{-1}}(D) = D^s \mathbf{I}_k$$

  for some $s \geq 0$
- A generator matrix $\mathbf{G}(D)$ is non-catastrophic $\iff$ it has a polynomial right pseudo inverse $\widetilde{\mathbf{G}^{-1}}(D)$
- A polynomial generator matrix $\mathbf{G}(D)$ has a polynomial right pseudo inverse $\iff$

$$\gcd\left\{\Delta_i(D), i = 1, 2, \ldots, \binom{n}{k}\right\} = D^s$$

  for some $s \geq 0$ where $\Delta_i(D), 1 \leq i \leq \binom{n}{k}$, are the determinants of the $\binom{n}{k}$ distinct $k \times k$ submatrices of $\mathbf{G}(D)$

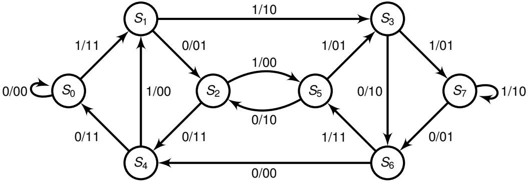
Free Distance

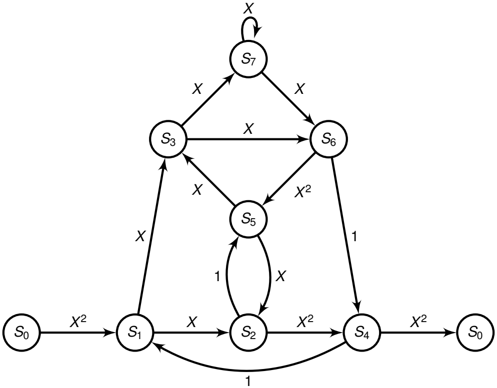
- The free distance of a convolutional code is the minimum Hamming distance between any two distinct codewords

$$d_{\text{free}} = \min_{\mathbf{v} \neq \mathbf{v}'} d_H(\mathbf{v}, \mathbf{v}') = \min_{\mathbf{v} \neq \mathbf{0}} w_H(\mathbf{v})$$

- It is assumed that $\mathbf{v}$ and $\mathbf{v}'$ start and end in the all-zeros state
- If $d_{\text{free}} \geq 2t + 1$, the convolutional code can correct all weight t error patterns

Calculating Free Distance





Questions? Takeaways?