Channel Coding Part I

Digital Communication
Chapter 6 & 7

Ola Jetlund

October 24, 2007

Introduction
Shannon
Linear Block Codes
Mapping
System model
Encoding
Decoding Linear block codes
Properties
Hamming codes
Convolutional Codes

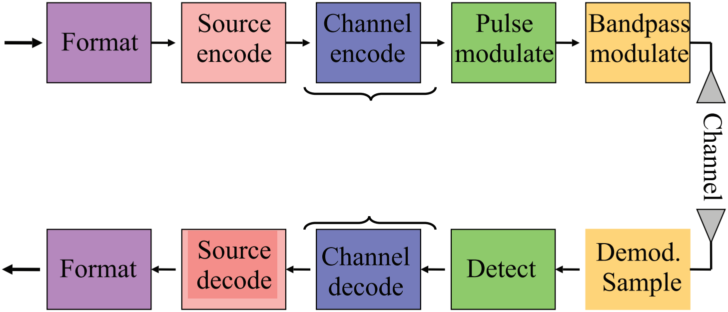
Last Week

- Evaluating the average probability of symbol error for different bandpass modulation schemes
- Comparing different modulation schemes based on their error performances.

This Week (and next week)

- Channel Coding
- Linear Block Codes
- Convolutional Codes

Digital Communication System



Introduction
Shannon
Linear Block Codes
Mapping
System model
Encoding
Decoding Linear block codes
Properties
Hamming codes
Convolutional Codes

Goals

For a DCS we can define the following goals:

- Maximizing the transmission bit rate
- Minimizing probability of bit error
- Minimizing the required power
- Minimizing required system bandwidth
- Maximizing system utilization
- Minimize system complexity

These are goals that must considered in the design phase.

Introduction

Shannon

Linear Block Codes

Mapping

System model

Encoding

Decoding Linear block codes

Properties

Hamming codes

Convolutional Codes

Channel Coding

- Transforming signals to improve communication performance
- Waveform coding
- Structured sequences

Error Control Techniques

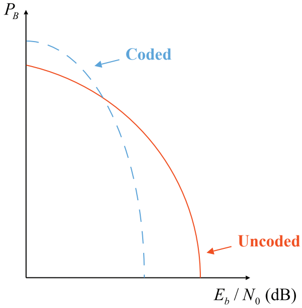
- ARQ - Automatic repeat request
- FEC - Forward Error Correction
- Hybrid ARQ - (ARQ + FEC)

Why error correcting codes?

- Error performance vs. bandwidth
- Power vs. bandwidth
- Data rate vs. bandwidth
- Capacity vs. bandwidth BP

CODING GAIN: Reduction in E_b/N_0 from using a code

$$G = \left(\frac{E_b}{N_0}\right)_u - \left(\frac{E_b}{N_0}\right)_c$$



Practical Channel coding

- Use as few bits as possible to transmit information on a noisy channel
- Decode received information with as few errors as possible

$\Rightarrow$ Utilize the channel capacity[1]:

$$C = W \log_2 \left(1 + \frac{S}{N}\right)$$

Here: capacity for an AWGN channel with:

- W Bandwidth [Hz]
- S Average received signal power
- N Average Noise power

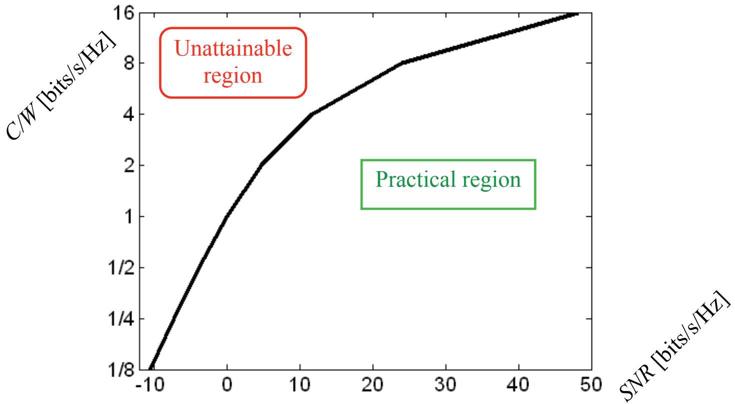
[1] C.E. Shannon, "A mathematical theory of communication," BSTJ, vol. 27, 1948, pp 379-423, 623-657.

Introduction
Shannon
Linear Block Codes
Mapping
System model
Encoding
Decoding Linear block codes
Properties
Hamming codes
Convolutional Codes

The Shannon theorem:

A limit on transmission data rate R_b

- Transmission with $R_b \leq C$ is possible
  - with an arbitrary small error probability
- For $R_b > C$, transmission cannot achieve an arbitrary small error probability.



The Shannon limit

$$\begin{aligned} C &= W \log_2\left(1+\frac{S}{N}\right) \\ S &= E_b C \\ N &= N_0 W \end{aligned} \quad \Rightarrow \quad \boxed{\frac{C}{W} = \log_2\left(1 + \frac{E_b}{N_0}\frac{C}{W}\right)}$$

As $W \to \infty$ or $\frac{C}{W} \to 0$,

$$\frac{E_b}{N_0} \to \frac{1}{\log_2(e)} = 0.693 \approx -1.6 \text{ [dB]}$$

- No error free transmission (at any rate) for $\frac{E_b}{N_0} < -1.6$ [dB]
- Capicity can be increased by increasing the bandwidth

Channel Coding Part I

Ola Jetlund

Introduction

Shannon

Linear Block Codes

Mapping

System model

Encoding

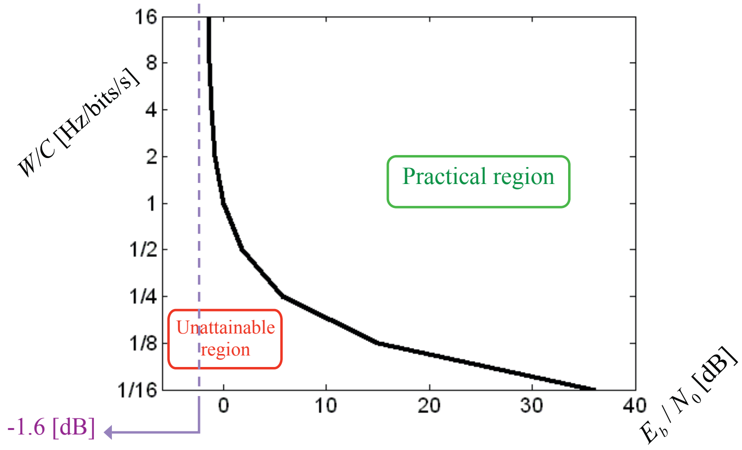
Decoding Linear block codes

Properties

Hamming codes

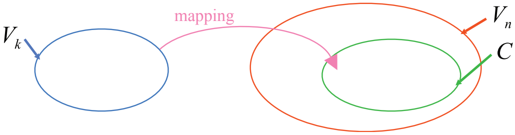
Convolutional Codes

The Shannon limit ...



Linear Block Codes (n, k), I

Coding is a mapping from one space to another:



V_m is a vector space containing all 2^k sequences of length m.

- A set $C \subset V_n$ with cardinality 2^k is called a linear block code if and only if it is a subspace of the vector space V_n.
  - Members of C are called codewords
  - The all-zero word is a codeword
  - any linear combination of a codeword is a codeword

Channel Coding Part I
Ola Jetlund
Introduction
Shannon
Linear Block Codes
Mapping
System model
Encoding
Decoding Linear block codes
Properties
Hamming codes
Convolutional Codes

A note on the binary field

- The set $\{0, 1\}$ under the modulo-2 binary addition and multiplication forms a field.

Addition	Multiplication
$0 \oplus 0 = 0$	$0 \otimes 0 = 0$
$0 \oplus 1 = 1$	$0 \otimes 1 = 0$
$1 \oplus 0 = 1$	$1 \otimes 0 = 0$
$1 \oplus 1 = 0$	$1 \otimes 1 = 1$

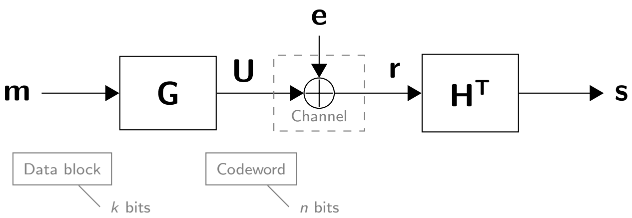
- AKA the Galois field: $\mathrm{GF}(2)$
- Example V_3

$$V_3 = \{(000),(001),(010),(011),\\ (100),(101),(110),(111)\}$$

It has $2^k = 2^3 = 8$ members (cardinality)

Introduction
Shannon
Linear Block Codes
Mapping
System model
Encoding
Decoding Linear block codes
Properties
Hamming codes
Convolutional Codes

Linear Block Codes (n, k), II



- **m** Message
- **G** Generator matrix
- **U** Codeword
- **e** Error introduced by channel
- **r** Received codeword
- **H** Parity check matrix
- **s** Syndrome (received data)

Note! We consider only binary sequences!

Introduction

Shannon

Linear Block Codes
- Mapping
- System model
- Encoding
- Decoding Linear block codes
- Properties
- Hamming codes

Convolutional Codes

- The (n, k) linear block code takes k data bit and produces a coded sequence of length n
  - $n - k$ parity bits
  - Code rate:

$$R_c = \frac{k}{n}$$

- Coding:

$$\mathbf{U} = \mathbf{m} \cdot \mathbf{G}$$

  The generator matrix $\mathbf{G}$ is of size $k \times n$ and it can be
  - systematic, or
  - nonsystematic.

Example, nonsystematic $(7,4)$

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \mathbf{g_1} \\ \mathbf{g_2} \\ \mathbf{g_3} \\ \mathbf{g_4} \end{bmatrix}$$

Given $\mathbf{m} = [1\,0\,0\,0]$, then

$$\mathbf{U} = \mathbf{d} \cdot \mathbf{G} = [1\,1\,0\,0\,0\,1\,0]$$

Note that all rows in $\mathbf{G}$ are codewords.

Remember: A linear combination of two codewords are a codeword

Thus we can manipulate G as follows:

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \mathbf{g_1} \\ \mathbf{g_2} \\ \mathbf{g_3} \\ \mathbf{g_4} \end{bmatrix}$$

$$\mathbf{g_5} = \mathbf{g_1} + \mathbf{g_2} = [1\,1\,0\,0\,0\,1\,0] + [0\,1\,0\,0\,1\,1\,1] = [1\,0\,0\,0\,1\,0\,1]$$

$$\mathbf{g_6} = \mathbf{g_3} + \mathbf{g_3} = [0\,0\,0\,1\,1\,1\,0] + [0\,0\,1\,1\,1\,1\,0] = [0\,0\,1\,0\,0\,0\,0]$$

Replace $\mathbf{g_1}$ with $\mathbf{g_5}$, $\mathbf{g_4}$ with $\mathbf{g_6}$ to obtain new generator matrix:

$$\mathbf{G}' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \mathbf{g_5} \\ \mathbf{g_2} \\ \mathbf{g_3} \\ \mathbf{g_6} \end{bmatrix}$$

Swap 3rd and 4th row in $\mathbf{G}'$ to obtain a new generator matrix:

$$\mathbf{G}'' = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

Note that

$$\mathbf{G}'' = \left[\ \mathbf{I}_4 \ \middle|\ \mathbf{P}\ \right]$$

Systematic block codes (n, k)

For a systematic code

- the first k bits are the information bits:

$$\mathbf{G} = \left[\ \mathbf{I}_k \ \middle|\ \mathbf{P}\ \right]$$

$\mathbf{I}_k$ is a $k \times k$ identity matrix
$\mathbf{P}$ is a $k \times (n-k)$ matrix

- Thus,

$$\begin{aligned}\mathbf{U} &= (u_1, u_2, \ldots, u_n) \\ &= (\overbrace{m_1, m_2, \ldots, m_k}^{\text{message bits}}, \overbrace{p_1, p_2, \ldots, p_{n-k}}^{\text{parity bits}})\end{aligned}$$

(Syndrom) Decoding I

For any linear block code with generator matrix $\mathbf{G}$ there exists a matrix $\mathbf{H}$ of size $(n-k) \times n$ such that

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$

- $\mathbf{H}$ is called the parity check matrix and its rows are linearly independent.
- For systematic linear block codes:

$$\mathbf{H} = \left[\begin{array}{c|c} \mathbf{P}^T & \mathbf{I}_{n-k} \end{array} \right]$$

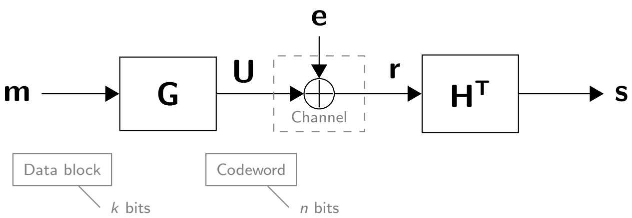
Introduction

Shannon

Linear Block Codes
- Mapping
- System model
- Encoding
- Decoding Linear block codes
- Properties
- Hamming codes

Convolutional Codes

Decoding II



$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T \qquad \mathbf{r} = \mathbf{U} + \mathbf{e} \qquad \mathbf{U} = \mathbf{m} \cdot \mathbf{G} \qquad \mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$

The syndrome $\mathbf{s}$:

$$\begin{aligned}\mathbf{s} &= \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{U} + \mathbf{e}) \cdot \mathbf{H}^T = (\mathbf{m} \cdot \mathbf{G} + \mathbf{e}) \cdot \mathbf{H}^T \\ &= \mathbf{m} \cdot \mathbf{G} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{m} \cdot \mathbf{0} + \mathbf{e} \cdot \mathbf{H}^T \\ &= \mathbf{0} + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T.\end{aligned}$$

Decoding III

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T$$

1. If $\mathbf{s} = \mathbf{0}$ then $\mathbf{r}$ is a legal codeword and the decoded message $\widehat{\mathbf{m}}$ is found from $\widehat{\mathbf{m}}\mathbf{G} = \mathbf{r}$,
2. and if $\mathbf{s} \neq \mathbf{0}$ then $\mathbf{r}$ is a not legal codeword.
   2.1 Find an error vector $\mathbf{e}'$ such that $\mathbf{r} - \mathbf{e}'$ is a legal codeword:

$$\text{Find } \mathbf{e}' \text{ such that } (\mathbf{r} - \mathbf{e}') \cdot \mathbf{H}^T = \mathbf{0}$$

Properties of linear block codes

For a (n, k) linear block code there are 2^k legal codewords: $\mathbf{U}_i,\ i \in 1, 2, \ldots 2^k$.

- Hamming weight: $w(\mathbf{U}_i) =$ the number of non-zero elements in $\mathbf{U}_i$.
- Hamming distance: $d(\mathbf{U}_i, \mathbf{U}_j) = w(\mathbf{U}_i \oplus \mathbf{U}_j)$
- Minimum distance:

$$d_{\min} = \min_{i \neq j} d(\mathbf{U}_i, \mathbf{U}_j) = \min_i w(\mathbf{U}_i)$$

A (n, k) linear block code can then

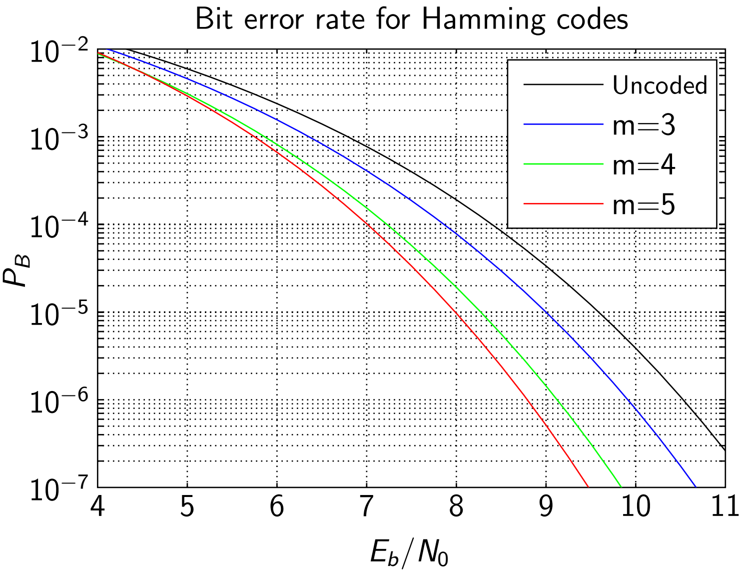
- Detect $e = d_{\min} - 1$ errors
- Correct $t = \lfloor \frac{d_{\min} - 1}{2} \rfloor$ errors

Example: Systematic Hamming code (m)

- Number of bits in codeword: $n = 2^m - 1$
- Number of information bits: $k = 2^m - m - 1$
- Number of parity bits: $n - k = m$
- Code rate $\frac{k}{n} = \frac{2^m - m - 1}{2^m - 1} = 1 - \frac{m}{2^m - 1}$

For Hamming codes the columns in **H** represents **all** binary vectors of length 2^{n-k} (except the all-zero codeword.

m	n	k
3	7	4
4	15	11
5	31	26

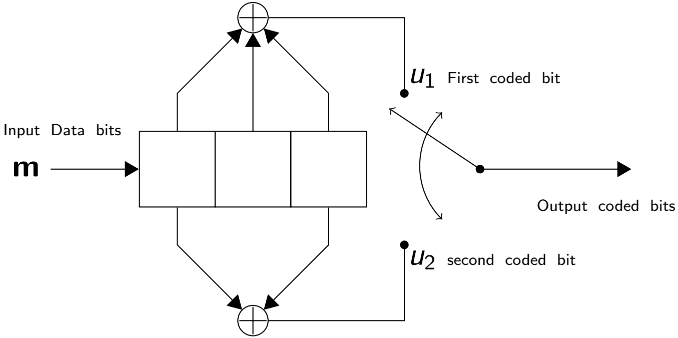

Bit error rate for Hamming codes
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
P_B
4
5
6
7
8
9
10
11
E_b/N_0
Uncoded
m=3
m=4
m=5

Convolution versus block encoding

- Linear block codes
  - Rate $R_c = \frac{k}{n}$
  - n is the length of the codewords
  - k is the length of the information sequence coded (or mapped) to one codeword
- Convolutional codes
  - Rate $R_c = \frac{k}{n}$
  - n does not define a block or a codeword
  - k usually set to 1
  - K constraint length - counting the number of memory elements (which is $K-1$)

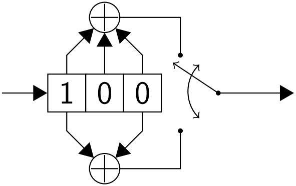
A convolutional code encodes the entire stream of data into a single codeword.

Example: Rate $R_c = \frac{1}{2}$

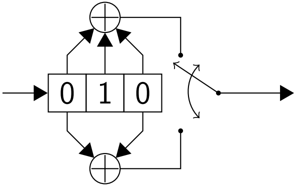


Here, $K = 3$

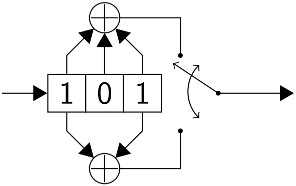
Let $\mathbf{m} = (101)$ and find the output.



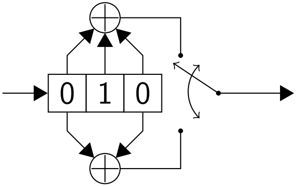
time t_1: $(u_1, u_2) = (1, 1)$



time t_2: $(u_1, u_2) = (1, 0)$



time t_3: $(u_1, u_2) = (0, 0)$



time t_4: $(u_1, u_2) = (1, 0)$

Introduction

Shannon

Linear Block Codes

Mapping

System model

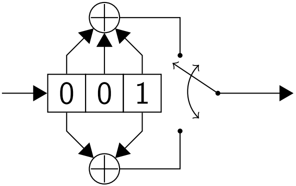
Encoding

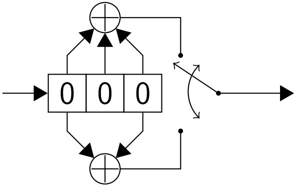
Decoding Linear block codes

Properties

Hamming codes

Convolutional Codes





time t_5: $(u_1, u_2) = (1, 1)$ time t_6: $(u_1, u_2) = (0, 0)$

$$\mathbf{m} = (101) \longrightarrow \boxed{\text{Encoder}} \longrightarrow \mathbf{U} = (11\ 10\ 00\ 10\ 11)$$

Description of convolutional codes

A Tree diagrams (not very common)

B State Diagram

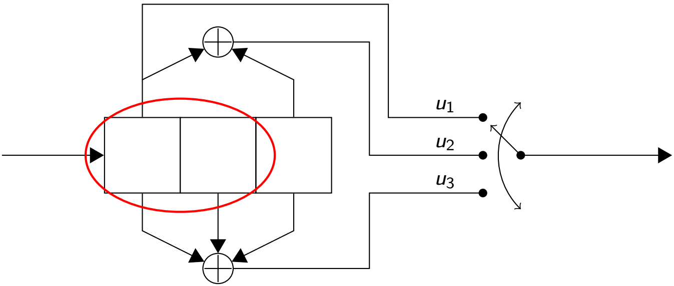
- Often used to find the exact error correcting properties of a code

C The trellis diagram

- Is often used to visualize the decoding process

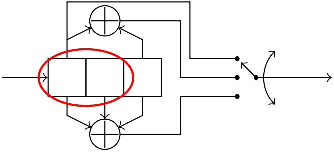
Another larger will illustrate descriptions B and C.

Example: $R_c = \frac{1}{3}$



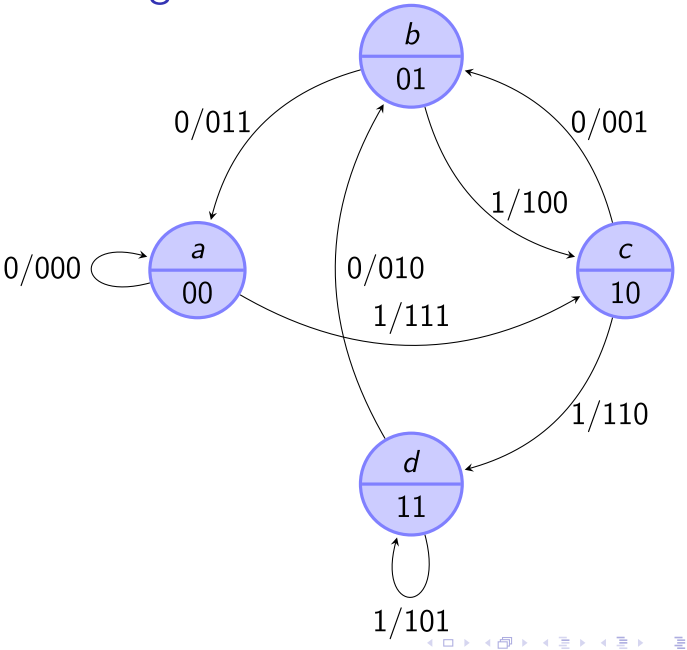
The State of a convolutional code are the $K-1$ first bits in the encoder

Inputs, states, and outputs

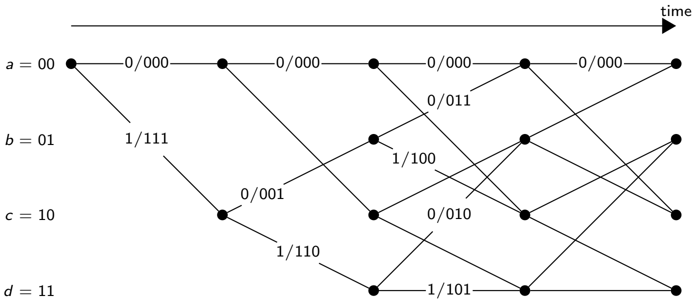


Input	Current State	Next State	Output	
0	0 0	0 0	0 0 0	"0"
1	0 0	1 0	1 1 1	"7"
0	0 1	0 0	0 1 1	"3"
1	0 1	1 0	1 0 0	"4"
0	1 0	0 1	0 0 1	"1"
1	1 0	1 1	1 1 0	"6"
0	1 1	0 1	0 1 0	"2"
1	1 1	1 1	1 0 1	"5"

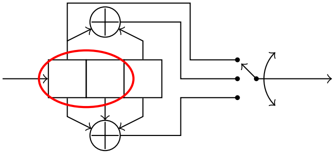
State Diagram

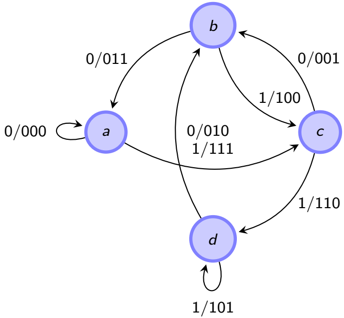


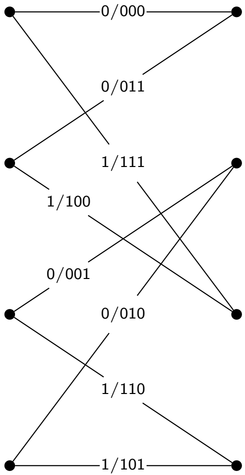
Trellis Diagram



Convolutional codes (block -, state -, and trellis diagram







Introduction

Shannon

Linear Block Codes

Mapping

System model

Encoding

Decoding Linear block codes

Properties

Hamming codes

Convolutional Codes

Introduction

Shannon

Linear Block Codes
- Mapping
- System model
- Encoding
- Decoding Linear block codes
- Properties
- Hamming codes

Convolutional Codes

Introduction

Shannon

Linear Block Codes
- Mapping
- System model
- Encoding
- Decoding Linear block codes
- Properties
- Hamming codes

Convolutional Codes

Introduction

Shannon

Linear Block Codes

Mapping

System model

Encoding

Decoding Linear block codes

Properties

Hamming codes

Convolutional Codes