Tutorials
Information Theory and Coding
SS2020

Institut für Nachrichtentechnik
Technische Universität Hamburg

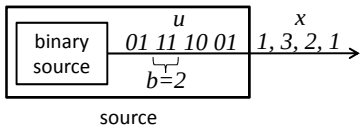
Contents

Chapter 1

Source Coding

1.1 Binary Source and Huffman Code

A binary source emits statistical independent binary data symbols $u \in \{0, 1\}$. The probability of a bit being "0 " is p_0, the probability of a bit "1 " is $p_1 = 1 - p_0$. Before compression, $b = 2$ data symbols u are grouped to a symbol x as depicted in the following figure:



Solve the following problems a)-c)for all parameter combinations

- $b = 2$ and $b = 3$
- $p_0 = 1/2$, $p_0 = 1/4$ and $p_0 = 2/5$.

a) Determine the probabilities $P_X(x)$ of all possible source symbols x.

Solution: (**b=2**)

	x			
p_0, p_1	0	1	2	3
$p_0 = \frac{1}{2} = p_1$	$p_0^2 = \frac{1}{4}$	$p_0 \cdot p_1 = \frac{1}{4}$	$p_0 \cdot p_1 = \frac{1}{4}$	$p_1^2 = \frac{1}{4}$
$p_0 = \frac{1}{4}, p_1 = \frac{3}{4}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{9}{16}$
$p_0 = \frac{2}{5}, p_1 = \frac{3}{5}$	$\frac{4}{25}$	$\frac{6}{25}$	$\frac{6}{25}$	$\frac{9}{25}$
	00	01	10	11
	u			

b) Determine the Entropy $H(X)$ of the source.

Solution: (**b=2**)

$$H(X) = \sum_x P(x) \log_2 \frac{1}{P(x)} = -\sum_x P(x) \log_2 P(x)$$

The entropy is the expected self information. It is a measure of uncertainty or loosely

speaking a "measure of surprise."

$$p_0 = \frac{1}{2}: \quad H(X) = 4 \cdot \frac{1}{4} \log_2(4) \text{ bit/symbol}$$
$$= 2 \text{ bit/symbol}$$
$$p_0 = \frac{1}{4}: \quad H(X) = \frac{1}{16} \log_2(16) \text{ bit/symbol} + 2 \cdot \frac{3}{16} \log_2\left(\frac{16}{3}\right) \text{ bit/symbol} + \frac{9}{16} \log_2\left(\frac{16}{9}\right) \text{ bit/symbol}$$
$$= 1.62 \text{ bit/symbol}$$
$$p_0 = \frac{2}{5}: \quad H(X) = \frac{4}{25} \log_2\left(\frac{25}{4}\right) \text{ bit/symbol} + 2 \cdot \frac{6}{25} \log_2\left(\frac{25}{6}\right) \text{ bit/symbol} + \frac{9}{25} \log_2\left(\frac{25}{9}\right) \text{ bit/symbol}$$
$$= 1.94 \text{ bit/symbol}$$

The maximum entropy is obtained for a uniform probability distribution $P_X(x)$, i.e. if all symbols x have the same probability.

Alternative solution:

$$H(X) = b \cdot H(U)$$

(since U is statistical independent).

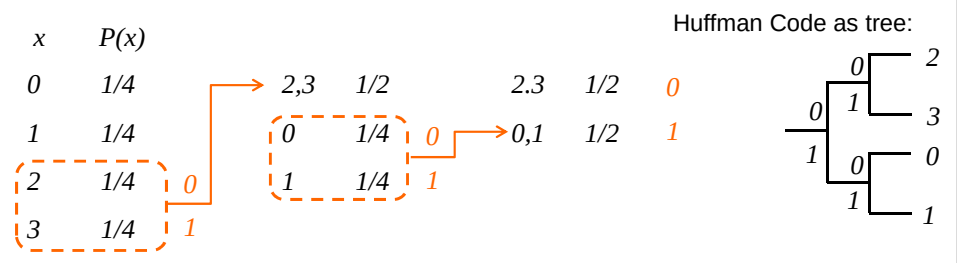
$$p_0 = \frac{1}{2}: \quad H(X) = b \cdot H(U) = 2 \cdot 2 \cdot \frac{1}{2} \log_2(2) \text{ bit/symbol}$$
$$= 2 \text{ bit/symbol}$$
$$p_0 = \frac{1}{4}: \quad H(X) = b \cdot H(U) = 2 \cdot \left(\frac{1}{4} \log_2(4) \text{ bit/symbol} + \frac{3}{4} \log_2\left(\frac{4}{3}\right) \text{ bit/symbol}\right)$$
$$= 1.62 \text{ bit/symbol}$$
$$p_0 = \frac{2}{5}: \quad H(X) = b \cdot H(U) = 2 \cdot \left(\frac{2}{5} \log_2(\frac{5}{2}) \text{ bit/symbol} + \frac{3}{5} \log_2\left(\frac{5}{3}\right) \text{ bit/symbol}\right)$$
$$= 1.94 \text{ bit/symbol}$$

c) State all possible Huffman Codes and

(1) calculate the average codeword length $\mu_L = E\{L\}$,
(2) calculate the variance σ_L^2 of the codeword length,
(3) compare the average codeword length $\mu_L = E\{L\}$ to the entropy $H(X)$ of the source.

Solution: (b=2)

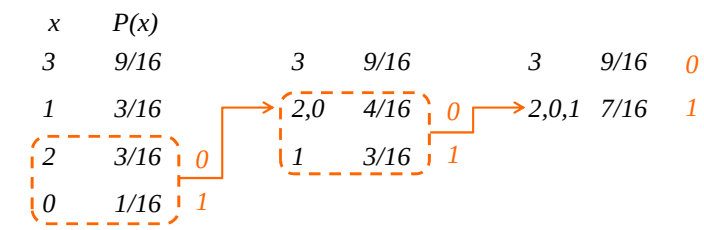
$p_0 = \frac{1}{2}$:

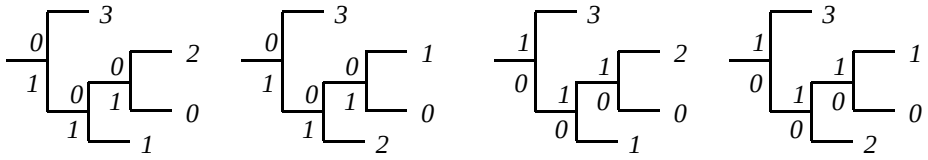


As all symbols x have the same probability $P_X(x)$, all symbols at the end of the Huffman tree can be exchanged arbitrarily. The equivalent Huffman codes result

formally by changing the sequence of the hyper symbols with same probability during construction or by interchanging the assignment of 0 and 1.

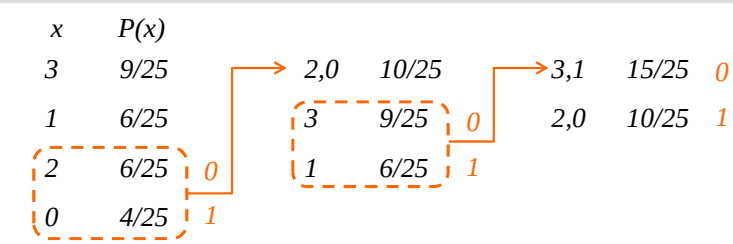
$p_0 = \frac{1}{4}$:

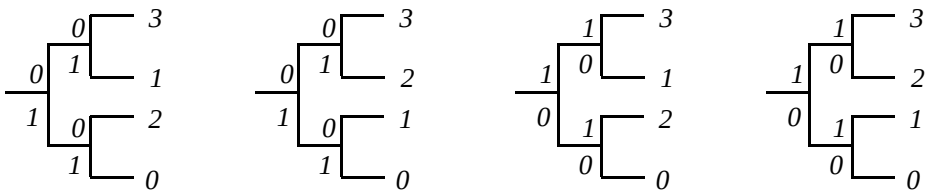




The probabilities of the symbols $x = 1$ and $x = 2$ are the same. Therefore, their position in the tree can be interchanged. The assignment of the bits 0 and 1 to the decisions at each branch is arbitrarily exchangeable.

$p_0 = \frac{2}{5}$:





The probabilities of the symbols $x = 1$ and $x = 2$ are the same. Therefore,their position in the tree can be interchanged. The assignment of the bits 0 and 1 to the decisions at each branch is arbitrarily exchangeable.

The mean codeword length is calculated as follows.

$$\mu_L = E\{L\} = \sum_x P(x)L(x)$$

$p_0 = \frac{1}{2}$:

$$\mu_L = 4 \cdot \frac{1}{4} \cdot 2 \text{ bit} = 2 \text{ bit} \quad \Rightarrow \text{ no compression}$$

$p_0 = \frac{1}{4}$:

$$\mu_L = \frac{9}{16} \cdot 1 \text{ bit} + \frac{3}{16} \cdot 2 \text{ bit} + \frac{3}{16} \cdot 3 \text{ bit} + \frac{1}{16} \cdot 3 \text{ bit} = 1.69 \text{ bit}$$

$p_0 = \frac{2}{5}$:

$$\mu_L = \frac{4}{25} \cdot 2 \text{ bit} + \frac{6}{25} \cdot 2 \text{ bit} + \frac{6}{25} \cdot 2 \text{ bit} + \frac{9}{25} \cdot 2 \text{ bit} = 2 \text{ bit}$$

The variance of the codeword length σ_L^2 is calculated as follows.

$$\sigma_L^2 = E\left\{\left(L^2(x) - \mu_L\right)^2\right\} = E\left\{L^2(x)\right\} - \mu_L^2 = \sum_x P(x) L^2(x) - \mu_L^2$$

$p_0 = \frac{1}{2}$:

$$\begin{aligned}\sigma_L^2 &= 4 \cdot \frac{1}{4} \cdot 2^2 \text{ bit}^2 - 2^2 \text{ bit}^2 \\ &= 0 \text{ bit}^2\end{aligned}$$

$p_0 = \frac{1}{4}$:

$$\begin{aligned}\sigma_L^2 &= \left(\frac{9}{16} \cdot 1^2 + \frac{3}{16} \cdot 2^2 + \frac{3}{16} \cdot 3^2 + \frac{1}{16} \cdot 3^2\right) \text{ bit}^2 - 1.69^2 \text{ bit}^2 \\ &= 0.71 \text{ bit}^2\end{aligned}$$

$p_0 = \frac{2}{5}$:

$$\sigma_L^2 = 0 \text{ bit}^2$$

Shannon's source coding theorem states that the average codeword length of binary source code is lower bounded by the entropy of the source:

$$H(X) \leq \mu_L$$

Equality is achieved by the Huffman code, if the probabilities $P_X(x)$ of all symbols x are a power of $\frac{1}{2}$. In this case, branch decisions in the Huffman tree which distinguish subtrees of probability $\frac{1}{2}$ are encoded by one bit, thus exactly according to their self information.

Furthermore, a source code can be found such that the average codeword length is bounded by

$$H(X) \leq \mu_L < H(X) + 1$$

$p_0 = \frac{1}{2}$:

$$\mu_L = 2 \text{ bit} = H(X)$$

$p_0 = \frac{1}{4}$:

$$H(X) = 1.62 \text{ bit} < \mu_L = 1.69 \text{ bit} < H(X) + 1 \text{ bit} = 2.62 \text{ bit}$$

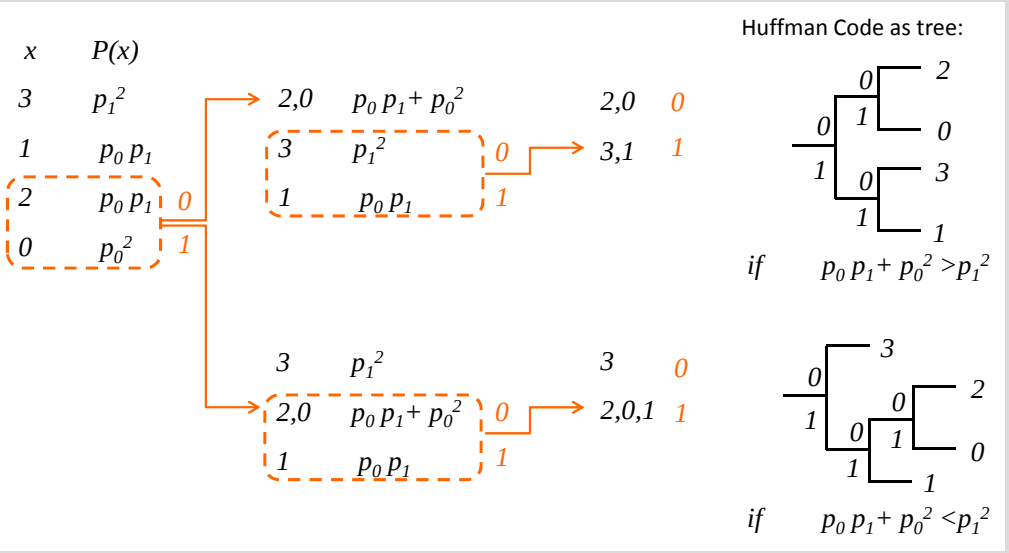
$p_0 = \frac{2}{5}$:

$$H(X) = 1.94 \text{ bit} < \mu_L = 2 \text{ bit} < H(X) + 1 \text{ bit} = 2.94 \text{ bit}$$

d) For $b = 2$, there exist two generally different Huffman-Codes. Determine the probability p_0, for which it is switched between both variants.

Solution: (b=2)

Assume $p_0 < p_1$:



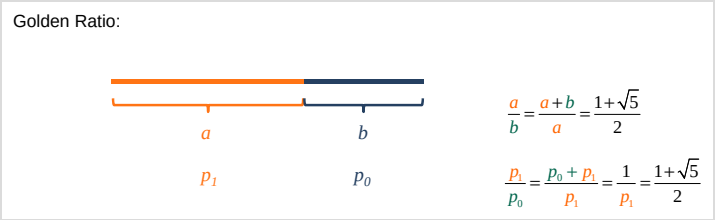
It is switched between both cases for $p_0 p_1 + p_0^2 = p_1^2$.

$$
\begin{aligned}
&\Leftrightarrow p_0(1-p_0) + p_0^2 = (1-p_0)^2 \\
&\Leftrightarrow p_0 - p_0^2 + p_0^2 = 1 - 2p_0 + p_0^2 \\
&\Leftrightarrow p_0^2 - 3p_0 + 1 = 0 \\
&\Rightarrow p_0 = \frac{3-\sqrt{9-4}}{2} = \frac{3-\sqrt{5}}{2} \\
&\Rightarrow p_1 = 1 - p_0 = \frac{-1+\sqrt{5}}{2}
\end{aligned}
$$

The ratio $\frac{p_1}{p_0} = \frac{1+\sqrt{5}}{2}$ corresponds exactly to the 'Golden ratio'.

$$
\frac{p_1}{p_0} = \frac{\frac{-1+\sqrt{5}}{2}}{\frac{3-\sqrt{5}}{2}} = \frac{(-1+\sqrt{5})(3+\sqrt{5})}{9-5} = \frac{-3+3\sqrt{5}-\sqrt{5}+5}{4} = \frac{1+\sqrt{5}}{2}
$$

$$
\frac{p_1+p_0}{p_0} = \frac{1}{p_1} = \frac{1}{\frac{-1+\sqrt{5}}{2}} = 2\frac{1+\sqrt{5}}{-1+5} = \frac{1+\sqrt{5}}{2}
$$



a) Determine the probabilities $P_X(x)$ of all possible source symbols x.

Solution: (**b=3**)

	x			
p_0, p_1	0	1	2	3
$p_0 = \frac{1}{2} = p_1$	$p_0^3 = \frac{1}{8}$	$p_0^2 \cdot p_1 = \frac{1}{8}$	$p_0^2 \cdot p_1 = \frac{1}{8}$	$p_0 \cdot p_1^2 = \frac{1}{8}$
$p_0 = \frac{1}{4}, p_1 = \frac{3}{4}$	$\frac{1}{64}$	$\frac{3}{64}$	$\frac{3}{64}$	$\frac{9}{64}$
$p_0 = \frac{2}{5}, p_1 = \frac{3}{5}$	$\frac{8}{125}$	$\frac{12}{125}$	$\frac{12}{125}$	$\frac{18}{125}$
	000	001	010	011
	u			

	x			
p_0, p_1	4	5	6	7
$p_0 = \frac{1}{2} = p_1$	$p_0^2 \cdot p_1 = \frac{1}{8}$	$p_0 \cdot p_1^2 = \frac{1}{8}$	$p_0 \cdot p_1^2 = \frac{1}{8}$	$p_1^3 = \frac{1}{8}$
$p_0 = \frac{1}{4}, p_1 = \frac{3}{4}$	$\frac{3}{64}$	$\frac{9}{64}$	$\frac{9}{64}$	$\frac{27}{64}$
$p_0 = \frac{2}{5}, p_1 = \frac{3}{5}$	$\frac{12}{125}$	$\frac{18}{125}$	$\frac{18}{125}$	$\frac{27}{125}$
	100	101	110	111
	u			

b) Determine the Entropy $H(X)$ of the source.

Solution: (**b=3**)

$$H(X) = \sum_x P(x) \log_2 \frac{1}{P(x)} = -\sum_x P(x) \log_2 P(x)$$

The entropy is the mean of the self information. It is "a measure of suprise".

$$\begin{aligned}
p_0 = \frac{1}{2}: \quad H(X) &= 8 \cdot \frac{1}{8} \log_2(8) \text{ bit} \\
&= 3 \text{ bit} \\
p_0 = \frac{1}{4}: \quad H(X) &= \frac{1}{64} \log_2(64) \text{ bit} + 3 \cdot \frac{3}{64} \log_2 \left(\frac{64}{3}\right) \text{ bit} \\
&\quad + 3 \cdot \frac{9}{64} \log_2 \left(\frac{64}{9}\right) \text{ bit} + \frac{27}{64} \log_2 \left(\frac{64}{27}\right) \text{ bit} \\
&= 2.43 \text{ bit} \\
p_0 = \frac{2}{5}: \quad H(X) &= \frac{8}{125} \log_2 \left(\frac{125}{8}\right) \text{ bit} + 3 \cdot \frac{12}{125} \log_2 \left(\frac{125}{12}\right) \text{ bit} \\
&\quad + 3 \cdot \frac{18}{125} \log_2 \left(\frac{125}{18}\right) \text{ bit} + \frac{27}{125} \log_2 \left(\frac{125}{27}\right) \text{ bit} \\
&= 2.91 \text{ bit}
\end{aligned}$$

c) State all possible Huffman Codes and

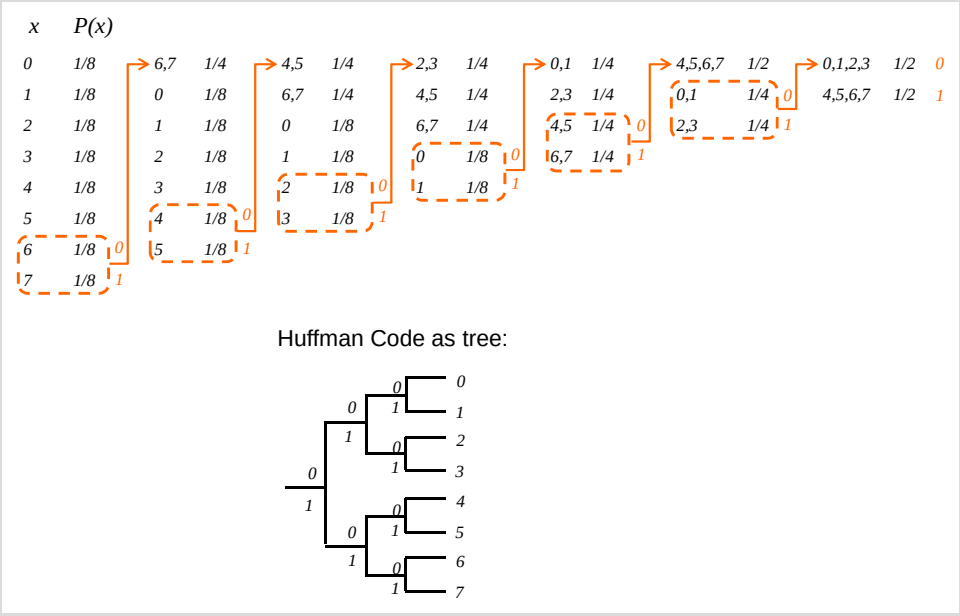
(1) calculate the average codeword length $\mu_L = E\{L\}$,

(2) calculate the variance σ_L^2 of the codeword length,

(3) compare the average codeword length $\mu_L = E\{L\}$ to the entropy $H(X)$ of the source.

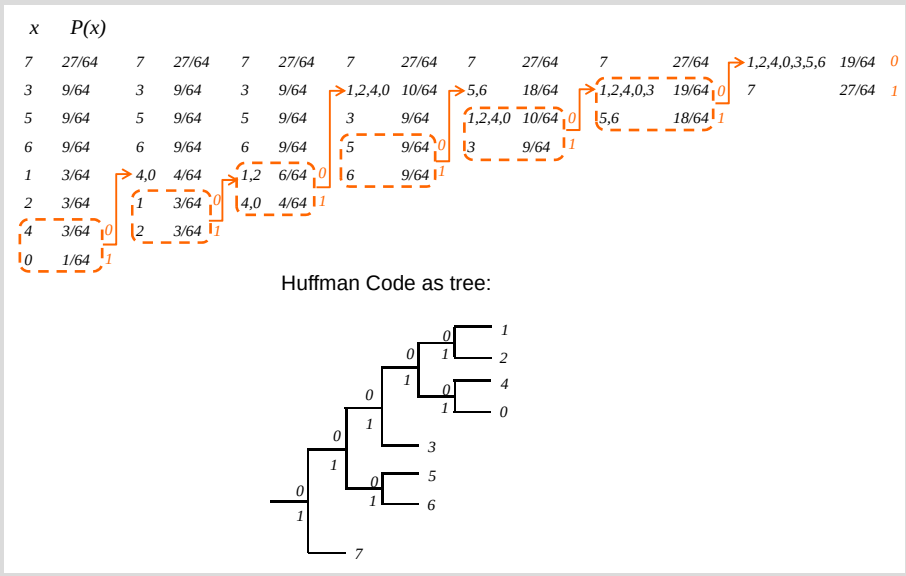
Solution: (b=3)

$p_0 = \frac{1}{2}$:



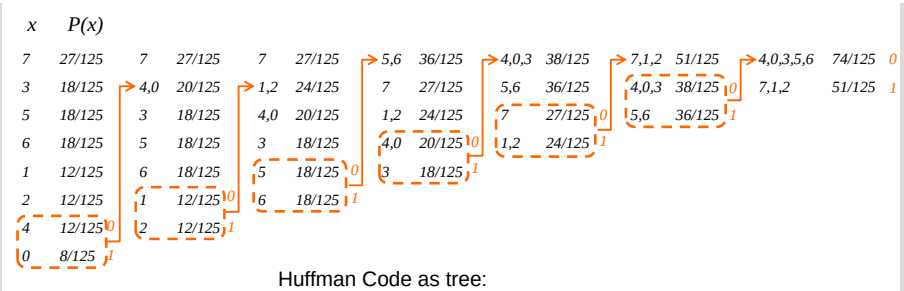
As all symbols x have the same probability $P(x)$, all symbols at the end of the Huffman tree can be exchanged arbitrarily. The equivalents Huffman codes result formally by changing the sequence of the hyper symbols of the construction.

$p_0 = \frac{1}{4}$:

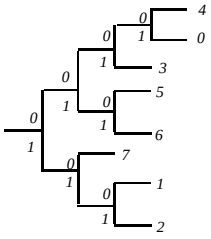


The equally likely symbols $1, 2, 4$ or $3, 5, 6$ are exchangeable among each other. The attribution of 0 and 1 to the branches of the tree is arbitrarily exchangeable. For the given probability distribution exists no Huffman code with different structure (that is for example with different variance of the codeword length).

$p_0 = \frac{2}{5}$:



Huffman Code as tree:



The equally likely symbols $1, 2, 4$ or $3, 5, 6$ are exchangeable among each other. The attribution of 0 and 1 to the branches of the tree is arbitrarily exchangeable. For the given probability distribution exists no Huffman code with different structure (that is for example with different variance of the codeword length).

The mean codeword length is calculated as follows.

$p_0 = \frac{1}{2}$:

$$\mu_L = 8 \cdot \frac{1}{8} \cdot 3 \text{ bit} = 3 \text{ bit} \quad \Rightarrow \text{ no compression}$$

$p_0 = \frac{1}{4}$:

$$\mu_L = \frac{27}{64} \cdot 1 \text{ bit} + 3 \cdot \frac{9}{64} \cdot 3 \text{ bit} + 3 \cdot \frac{3}{64} \cdot 5 \text{ bit} + 1 \cdot \frac{1}{64} \cdot 5 \text{ bit} = 2.47 \text{ bit}$$

$p_0 = \frac{2}{5}$:

$$\mu_L = 1 \cdot \frac{27}{125} \cdot 2 \text{ bit} + 3 \cdot \frac{18}{125} \cdot 3 \text{ bit} + 2 \cdot \frac{12}{125} \cdot 3 \text{ bit} + \frac{12}{125} \cdot 4 \text{ bit} + \frac{8}{125} \cdot 4 \text{ bit} = 2.94 \text{ bit}$$

The variance of the codeword length σ_L^2 is calculated as follows.

$p_0 = \frac{1}{2}$:

$$\begin{aligned} \sigma_L^2 &= \sum_x P(x) L^2(x) - \mu_L^2 = 8 \cdot \frac{1}{8} \cdot 3^2 \text{ bit}^2 - 3^2 \text{ bit}^2 \\ &= 0 \text{ bit}^2 \end{aligned}$$

$p_0 = \frac{1}{4}$:

$$\begin{aligned} \sigma_L^2 &= \left(\frac{27}{64} \cdot 1^2 + 3 \cdot \frac{9}{64} \cdot 3^2 + 3 \cdot \frac{3}{64} \cdot 5^2 + 1 \cdot \frac{1}{64} \cdot 5^2 \right) \text{ bit}^2 - 2.47^2 \text{ bit}^2 \\ &= 2.01 \text{ bit}^2 \end{aligned}$$

$p_0 = \frac{2}{5}$:

$$\sigma_L^2 = \left(\frac{27}{125} \cdot 2^2 + 3 \cdot \frac{18}{125} \cdot 3^2 + 2 \cdot \frac{12}{125} \cdot 3^2 + \frac{12}{125} \cdot 4^2 + \frac{8}{125} \cdot 4^2 \right) \text{ bit}^2 - 2.94^2 \text{ bit}^2$$
$$= 0.37 \text{ bit}^2$$

Comparison of the mean codeword length and the entropy of the source.

$p_0 = \frac{1}{2}$:

$$\mu_L = 3 \text{ bit} = H(X)$$

$p_0 = \frac{1}{4}$:

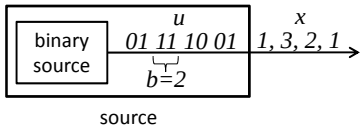
$$H(X) = 2.43 \text{ bit} < \mu_L = 2.47 \text{ bit} < H(X) + 1 \text{ bit} = 3.43 \text{ bit}$$

$p_0 = \frac{2}{5}$:

$$H(X) = 2.91 \text{ bit} < \mu_L = 2.94 \text{ bit} < H(X) + 1 \text{ bit} = 3.91 \text{ bit}$$

1.2 Fano Code

A binary source emits statistical independent binary data symbols $u \in \{0, 1\}$. The probability of a bit being "0 " is p_0, the probability of a bit "1 " is $p_1 = 1 - p_0$. Before compression, $b = 2$ data symbols u are grouped to a symbol x as depicted in the following figure:



Solve the following problems a)-c)for all parameter combinations

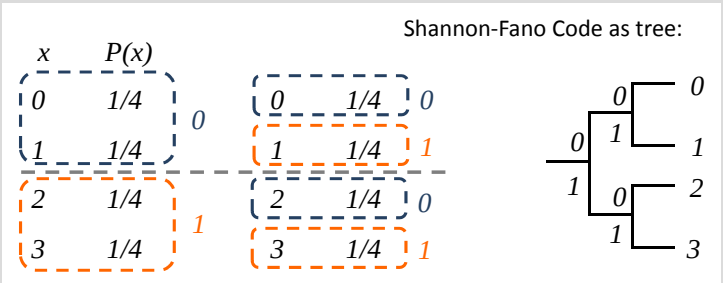
- $b = 2$ and $b = 3$
- $p_0 = 1/2$, $p_0 = 1/4$ and $p_0 = 2/5$.

a) State all possible Fano Codes and

(1) calculate the average codeword length $\mu_L = E\{L\}$,
(2) calculate the variance σ_L^2 of the codeword length,
(3) compare the average codeword length $\mu_L = E\{L\}$ to the entropy $H(X)$ of the source.

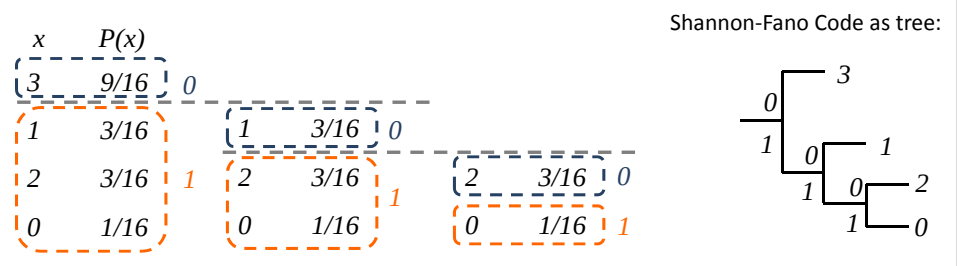
Solution: (b=2)

$p_0 = \frac{1}{2}$:

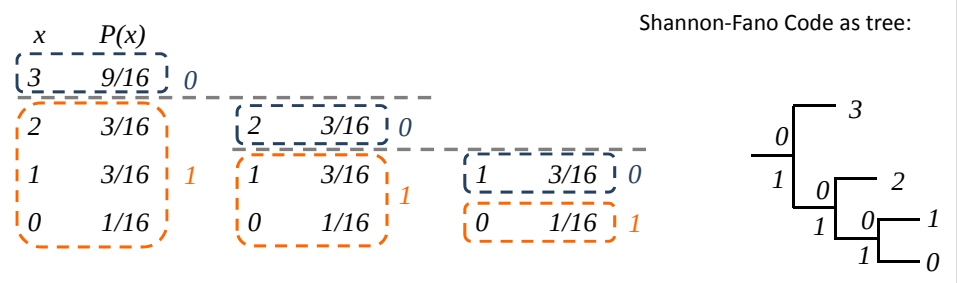


As all symbols x are equally likely, all symbols in the Fano tree are arbitrarily exchangeable. Equivalent Fano codes result by changing the composition of the groups with same probability.

$p_0 = \frac{1}{4}$:

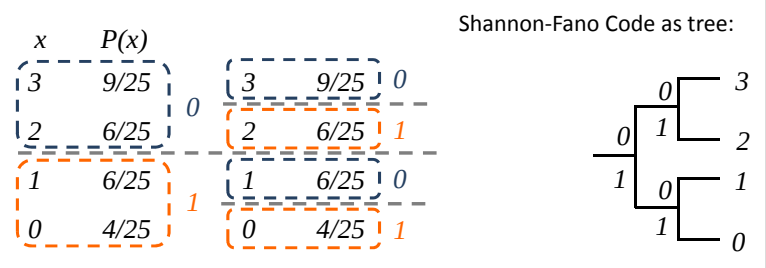


Alternative:



The assignment of 0 and 1 is chosen arbitrarily in each construction step.

$p_0 = \frac{2}{5}$:



The assignment of 0 and 1 is chosen arbitrarily in each construction step.

The mean codeword length μ_L is calculated as follows.

$$\mu_L = E\{L\} = \sum_x P(x)L(x)$$

$p_0 = \frac{1}{2}$:

$$\mu_L = 4 \cdot \frac{1}{4} \cdot 2 \text{ bit} = 2 \text{ bit} \quad \Rightarrow \text{ no compression!}$$

$p_0 = \frac{1}{4}$:

$$\mu_L = \frac{9}{16} \cdot 1 \text{ bit} + 2 \cdot \frac{3}{16} \cdot 2 \text{ bit} + \frac{3}{16} \cdot 3 \text{ bit} + \frac{1}{16} \cdot 3 \text{ bit} = 1.69 \text{ bit}$$

$p_0 = \frac{2}{5}$:

$$\mu_L = \frac{9}{25} \cdot 2 \text{ bit} + 2 \cdot \frac{6}{25} \cdot 2 \text{ bit} + \frac{4}{25} \cdot 2 \text{ bit} = 2 \text{ bit} \quad \Rightarrow \text{ no compression!}$$

The variance of the codeword length σ_L^2 is calculated as follows.

$$\sigma_L^2 = E\left\{\left(L^2(x) - \mu_L\right)^2\right\} = E\left\{L^2(x)\right\} - \mu_L^2 = \sum_x P(x)L^2(x) - \mu_L^2$$

$p_0 = \frac{1}{2}$:

$$\begin{aligned}\sigma_L^2 &= 4 \cdot \frac{1}{4} \cdot 2^2 \text{ bit}^2 - 2^2 \text{ bit}^2 \\ &= 0 \text{ bit}^2\end{aligned}$$

$p_0 = \frac{1}{4}$:

$$\sigma_L^2 = \frac{9}{16} \cdot 1^2 \text{ bit}^2 + 2 \cdot \frac{3}{16} \cdot 2^2 \text{ bit}^2 + \frac{3}{16} \cdot 3^2 \text{ bit}^2 + \frac{1}{16} \cdot 3^2 \text{ bit}^{\ 2} - 1.69^2 \text{ bit}^2 \quad = 0.71 \text{ bit}^2$$

$p_0 = \frac{2}{5}$:

$$\begin{aligned}\sigma_L^2 &= \frac{9}{25} \cdot 2^2 \text{ bit}^2 + 2 \cdot \frac{6}{25} \cdot 2^2 \text{ bit}^2 + \frac{4}{25} \cdot 2^2 \text{ bit}^2 - 2^2 \text{ bit}^2 \\ &= 0 \text{ bit}^2\end{aligned}$$

Comparison of the mean codeword length $\mu_L = E\{L\}$ with the entropy $H(X)$ of the source:

p_0	$H(X)$	μ_L		σ_L^2	
		Huffman	Fano	Huffman	Fano
$\frac{1}{2}$	2.00 bit	2.00 bit	2.00 bit	0.00 bit^2	0.00 bit^2
$\frac{1}{4}$	1.62 bit	1.69 bit	1.69 bit	0.71 bit^2	0.71 bit^2
$\frac{2}{5}$	1.94 bit	2.00 bit	2.00 bit	0.00 bit^2	0.00 bit^2

In the first case - $p_0 = 1/2$ - the entropy equal the length of a data symbol $H(X) = b = 2$ bits. No compression can be achieved in that case. The entropy of the 2nd and 3rd case - $p_0 = 1/4$ and $p_0 = 2/5$ - is smaller than the length of a data symbol $H(X)$ ¡ $b = 2$ bits. Compression could be achieved in these cases. However, compression is achieved only in the second case (Huffman $\mu_L = 1.69$,Fano $\mu_L = 1.69$). For the third case, no compression can be achieved with the Huffman and Fano code.

a) State all possible Fano Codes and

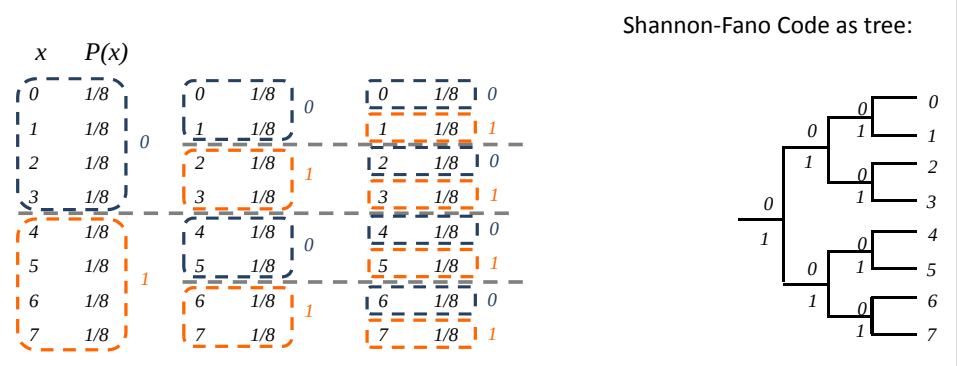
(1) calculate the average codeword length $\mu_L = E\{L\}$,

(2) calculate the variance σ_L^2 of the codeword length,

(3) compare the average codeword length $\mu_L = E\{L\}$ to the entropy $H(X)$ of the source.

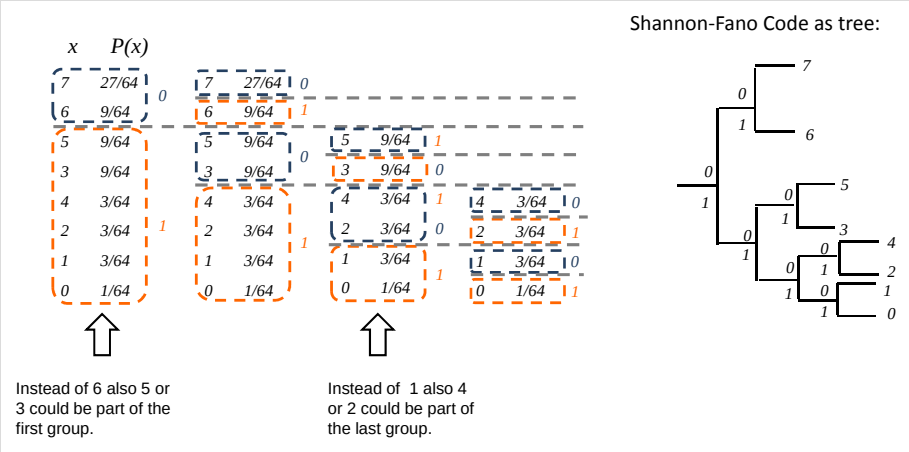
Solution: (**b=3**)

$p_0 = \frac{1}{2}$:



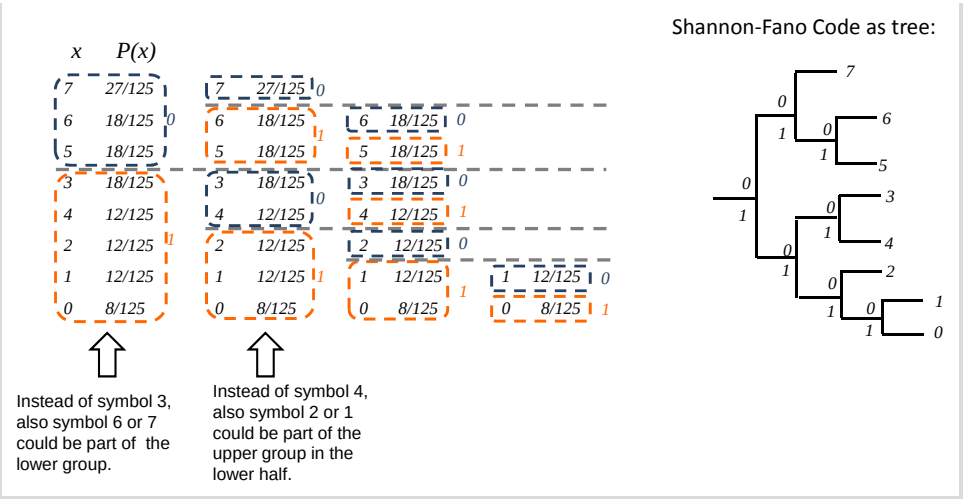
As all symbols x are equally likely $P(x)$, all symbols at the end of each branch of the Fano tree are arbitrarily exchangeable. The equivalent Fano codes result by changing the composition of the groups with same probability.

$p_0 = \frac{1}{2}$:



The attribution of 0 and 1 is chosen arbitrarily in the each construction step.

$p_0 = \frac{2}{5}$:



The attribution of 0 and 1 is chosen arbitrarily in the each construction step. The mean codeword length μ_L is calculated as follows.

$p_0 = \frac{1}{2}$:

$$\mu_L = 8 \cdot \frac{1}{8} \cdot 3 \text{ bit} = 3 \text{ bit} \quad \Rightarrow \text{ no compression!}$$

$p_0 = \frac{1}{4}$:

$$\mu_L = \frac{27}{64} \cdot 2 \text{ bit} + \frac{9}{64} \cdot 2 \text{ bit} + 2 \cdot \frac{9}{64} \cdot 3 \text{ bit} + 3 \cdot \frac{3}{64} \cdot 4 \text{ bit} + \frac{1}{64} \cdot 4 \text{ bit} = 2.59 \text{ bit}$$

$p_0 = \frac{2}{5}$:

$$\mu_L = \frac{27}{125} \cdot 2 \text{ bit} + 3 \cdot \frac{18}{125} \cdot 3 \text{ bit} + 2 \cdot \frac{12}{125} \cdot 3 \text{ bit} + \frac{12}{125} \cdot 4 \text{ bit} + \frac{8}{125} \cdot 4 \text{ bit} = 2.944 \text{ bit}$$

The variance of the codeword length σ_L^2 is calculated as follows.

$p_0 = \frac{1}{2}$:

$$\begin{aligned} \sigma_L^2 &= 8 \cdot \frac{1}{8} \cdot 3^2 \text{ bit}^2 - 3^2 \text{ bit}^2 \\ &= 0 \text{ bit}^2 \end{aligned}$$

$p_0 = \frac{1}{4}$:

$$\begin{aligned} \sigma_L^2 &= \frac{27}{64} \cdot 2^2 \text{ bit}^2 + \frac{9}{64} \cdot 2^2 \text{ bit}^2 + 2 \cdot \frac{9}{64} \cdot 3^2 \text{ bit}^2 + 3 \cdot \frac{3}{64} \cdot 4^2 \text{ bit}^2 + \frac{1}{64} \cdot 4^2 \text{ bit}^2 - 2.59^2 \text{ bit}^2 \\ &= 0.57 \text{ bit}^2 \end{aligned}$$

$p_0 = \frac{2}{5}$:

$$\begin{aligned} \sigma_L^2 &= \frac{27}{125} \cdot 2^2 \text{ bit}^2 + 3 \cdot \frac{18}{125} \cdot 3^2 \text{ bit}^2 + 2 \cdot \frac{12}{125} \cdot 3^2 \text{ bit}^2 + \frac{12}{125} \cdot 4^2 \text{ bit}^2 + \frac{8}{125} \cdot 4^2 \text{ bit}^2 - 2.944^2 \text{ bit}^2 \\ &= 0.37 \text{ bit}^2 \end{aligned}$$

Comparison of the mean codeword length $\mu_L = E\{L\}$ with the entropy $H(X)$ of the source:

p_0	$H(X)$	μ_L		σ_L^2	
		Huffman	Fano	Huffman	Fano
$\frac{1}{2}$	3.00 bit	3.00 bit	3.00 bit	0.00 bit^2	0.00 bit^2
$\frac{1}{4}$	2.43 bit	2.47 bit	2.59 bit	2.03 bit^2	0.57 bit^2
$\frac{2}{5}$	2.91 bit	2.94 bit	2.94 bit	0.37 bit^2	0.37 bit^2

The mean codeword length of the Fano code reaches the entropy of the source, if in each construction step the two groups are equally likely.

1.3 Huffman Code and Relative Entropy

Consider a 4-ary random variable X with realizations $x \in \{a, b, c, d\}$. The true probability distribution $p(x)$ is given in the following table:

x	$P(X = x)$
a	1/2
b	1/4
c	1/8
d	1/8

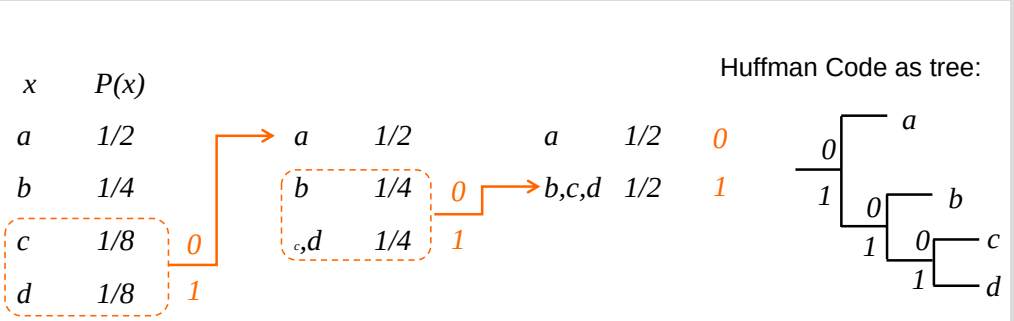
a) Determine the entropy $H(X)$ of the random variable X.

Solution:

$$H(x) = \sum_x p(x) \log_2 \frac{1}{p(x)} = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + 2 \cdot \frac{1}{8}\log_2 8$$
$$= \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{4}$$
$$= \frac{7}{4}\text{bit/symbol}$$

b) Construct a Huffman-Code for binary encoding of the realizations x. Make sure that all steps in the construction of the Huffman code are clearly given. Represent the mapping of realizations x to codewords c of the Huffman code in a table.

Solution:



c) Determine the average codeword length of the Huffman code from b).

Solution:

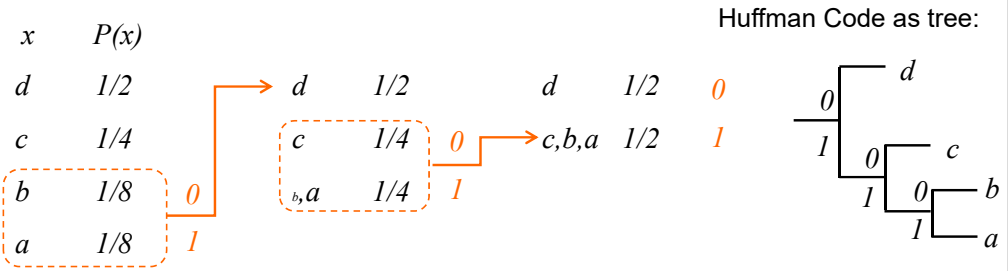
$$E\{L\} = \sum_x P(x) \cdot L(x) = P(X = a) \cdot 1 + P(X = b) \cdot 2 + P(X = c) \cdot 3 + P(X = d) \cdot 3$$
$$= \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \cdot \frac{1}{8} \cdot 3$$
$$= 1.75\text{bit/symbol}$$

Construction of a Huffman code requires knowledge of the statistics of the random variable X. Often, the probability distribution $p(x)$ of the random variable X is not exactly known but has to be estimated. Assume, that a probability distribution $q(x)$ according to the following table has been estimated instead of the true probability distribution $p(x)$:

x	$q(x)$
a	1/8
b	1/8
c	1/4
d	1/2

d) Construct a Huffman code for X based on the estimated probabilities $q(x)$. Represent the mapping of realizations x to codewords $\mathbf{w}$ of the Huffman code in a table.

Solution:



e) Determine the average codeword length of the Huffman code from d) and compare to your result from c).

Solution:

$$E\{L\} = \sum_x p(x) \cdot \tilde{L}(x) = P(X=a)\cdot 3 + P(X=b)\cdot 3 + P(X=c)\cdot 2 + P(X=d)\cdot 1$$
$$= \frac{1}{2}\cdot 3 + \frac{1}{4}\cdot 3 + \frac{1}{8}\cdot 2 + \cdot\frac{1}{8}\cdot 1$$
$$= 2.625\text{bit/symbol} > 1.75\text{bit/symbol}$$

The average codeword length is larger than for the Huffman Code from b)/c).

Assume that the source emits the symbol sequence b, c, a, c, d.

f) Determine the coded bit sequence.

Solution: Using the code constructed in b), b is assigned to "10", c to "110", a to "0" and d to "111". Therefore, the corresponding bit sequence is

10 110 0 110 111

g) Assume that due to a transmission error, the fourth bit in the coded sequence has been corrupted. Decode the erroneous bit sequence. Which fundamental problem of the Huffman code do you identify?

Solution: Due to the error, the erroneous bit sequence is

$$10\ 100\ 0\ 110\ 111$$

Decoding leads to

$$a\ b\ a\ a\ c\ d.$$

The bit error leads to several symbol errors. This is known as error propagation. In this example, even the number of detected symbols is wrong.

The distance of two probability distributions $p(x)$ and $q_X(x)$ can be measured by the *relative entropy*

$$D(p||q) = \sum_x p(x) \log_2 \frac{p(x)}{q(x)}$$

which is also called the Kullback Leibler distance.

h) Determine the relative entropy $D(p||q)$ of the probability distributions $p(x)$ and $q(x)$.

Solution:

$$\begin{aligned} D(p||q) &= \sum_x p(x) \log_2 \frac{p(x)}{q(x)} \\ &= P(X=a) \log_2 \frac{P(X=a)}{Q(X=a)} + P(X=b) \log_2 \frac{P(X=b)}{Q(X=b)} \\ &+ P(X=c) \log_2 \frac{P(X=c)}{Q(X=c)} + P(X=d) \log_2 \frac{P(X=d)}{Q(X=d)} \\ &= \frac{1}{2} \log_2 \frac{1/2}{1/8} + \frac{1}{4} \log_2 \frac{1/4}{1/8} \\ &+ \frac{1}{8} \log_2 \frac{1/8}{1/4} + \frac{1}{8} \log_2 \frac{1/8}{1/2} \\ &= \frac{7}{8} \text{bit} \end{aligned}$$

i) Interpret the meaning of the relative entropy for compression in view of your results for problems a)-e).

Solution:

The average codeword length of the Huffman code from d), which was constructed based on the wrong probability distribution $q_X(x)$, is given by $E\{L\} = H(X) + D(p||q) = \frac{7}{4} + \frac{7}{8} = \frac{21}{8}$ bit/symbol. The relative entropy $D(p||q)$ is the penalty in terms of the achievable codeword length when using the wrong probability distribution $q_X(x)$ instead of the true probability distribution $p_X(x)$ for the Huffman code construction.

j) Show, that the relative entropy $D(p||q)$ is always non-negative.

Help: Jensen's inequality: $E\{f(X)\} \leq f(E\{X\})$ for a concave function $f(\cdot)$ and a random variable X, where $E\{\cdot\}$ denotes expectation.

Solution:

$$
\begin{aligned}
D(p||q) &= \sum_x p(x) \log_2 \frac{p(x)}{q(x)} \\
-D(p||q) &= \sum_x p_X(x) \log_2 \frac{q(x)}{p(x)} \\
&= E_X \left\{ \log_2 \frac{q(x)}{p(x)} \right\} \\
&\leq \log_2 \left(E_X \left\{ \frac{q(x)}{p(x)} \right\} \right) \\
&= \log_2 \left(\sum_x p(x) \frac{q(x)}{p(x)} \right) \\
&= \log_2 \left(\sum_x q(x) \right) \\
&= \log_2(1) = 0
\end{aligned}
$$

$$
\begin{aligned}
&\Rightarrow -D(p||q) \leq 0 \\
&\Rightarrow D(p||q) \geq 0
\end{aligned}
$$

k) Derive the relation between $p(x)$ and $q(x)$ for which the relative entropy is zero, i.e. $D(p||q) = 0$.

Solution:

$$
\begin{aligned}
\log_2 \frac{p(x)}{q(x)} &= 0 \quad \text{for } p(x) = q(x) \\
\Rightarrow D(p||q) &= 0 \quad \text{for } p(x) = q(x) \forall x
\end{aligned}
$$

l) Is the relative entropy in general a true distance in the sense that it is symmetric, i.e. does $D(p||q) = D(q||p)$ hold for arbitrary probability distributions $p(x)$ and $q(x)$?

Solution:

$$
\begin{aligned}
D(p||q) &= \sum_x p(x) \log_2 \frac{p(x)}{q(x)} \\
&\neq \sum_x q(x) \log_2 \frac{q(x)}{p(x)} = D(q||p)
\end{aligned}
$$

The relative entropy is not symmetric and, therefore, is actually not a true distance.

n) Assume that a sequence of b independent realizations of X, i.e. $(x_1, x_2, \ldots, x_b)$, is mapped onto a distinct hyper symbol S. Compute the ratio between the entropy of a single symbol $H(X)$ and the entropy of a hyper symbol $H(S)$.

Solution:

The probability $p(s)$ of the hyper symbol equals the joint probability of the corresponding sequence, i.e. $p(x_1, x_2, \ldots, x_b)$.

Due to the assumed independence, $p(x_1, x_2, \ldots, x_b)$ can be written as

$$p(x_1, x_2, \ldots, x_b) = p(x_1) \cdot p(x_1) \cdot \ldots \cdot p(x_b).$$

In a next step, we exploit the correspondence between sequence and hyper symbol to compute the entropy $H(S)$.

Thus, instead of computing

$$H(S) = \sum_s p(s) \log_2 \frac{1}{p(s)},$$

$H(X_1, X_2, \ldots, X_b)$ is determined as

$$\begin{aligned}
H(X_1, X_2, \ldots, X_b) &= \sum_{x_1} \sum_{x_2} \cdots \sum_{x_b} p(x_1, x_2, \ldots, x_b) \log_2 \frac{1}{p(x_1, x_2, \ldots, x_b)} \\
&= \sum_{x_1} \sum_{x_2} \cdots \sum_{x_b} p(x_1) \cdot p(x_2) \cdot \ldots \cdot p(x_b) \log_2 \frac{1}{p(x_1) \cdot p(x_2) \cdot \ldots \cdot p(x_b)} \\
&= \sum_{x_1} \sum_{x_2} \cdots \sum_{x_b} p(x_1) \cdot p(x_2) \cdot \ldots \cdot p(x_b) \\
&\quad \cdot \left(\log_2 \frac{1}{p(x_1)} + \log_2 \frac{1}{p(x_2)} + \cdots + \log_2 \frac{1}{p(x_b)} \right) \\
&= \sum_{x_1} p(x_1) \log_2 \frac{1}{p(x_1)} + \sum_{x_2} \log_2 \frac{1}{p(x_2)} + \cdots + \sum_{x_b} p(x_b) \log_2 \frac{1}{p(x_b)} \\
&= H(X_1) + H(X_2) + \cdots + H(X_b) \\
&= b \cdot H(X) = H(S).
\end{aligned}$$

Therefore, the ratio between $H(S)$ and $H(X)$ is b, i.e. the length of the sequence mapped onto a hyper symbol.

Chapter 2

Entropy and Mutual Information

2.1 Mutual Information

Show that the mutual information between two random variables X and Y can be expressed by

$$I(X;Y) = H(Y) - H(Y|X) = H(X) - H(X|Y),$$

where $H(Y)$ and $H(Y|X)$ denote the entropy of Y and the conditional entropy of Y given X, respectively.

Solution:

Mutual information is the amount of uncertainty about x that is removed by knowing y and vice versa.
In the following, we show the proof of $I(X,Y) = H(Y) - H(Y|X)$.

$$\begin{aligned}
I(X;Y) &= \sum_x \sum_y p(x,y) \log_2 \left(\frac{p(x,y)}{p(x)p(y)} \right) \\
&= \sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(y)} \right) + p(x,y) \log_2 \left(\frac{p(x,y)}{p(x)} \right) \\
&= \left[\sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(y)} \right) \right] + \left[\sum_x \sum_y p(x,y) \log_2 \left(\frac{p(x,y)}{p(x)} \right) \right] \\
&= \left[\sum_y \underbrace{\left[\sum_x p(x,y) \right]}_{p(y)} \log_2 \left(\frac{1}{p(y)} \right) \right] + \left[\sum_x \sum_y p(x,y) \log_2 \left(p(y|x) \right) \right] \\
&= H(Y) - \sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(y|x)} \right) \\
&= H(Y) - H(Y|X)
\end{aligned}$$

Analogeously, it can be shown that $I(X,Y) = H(X) - H(X|Y)$.

$$\begin{aligned}
I(X;Y) &= \sum_x \sum_y p(x,y) \log_2 \left(\frac{p(x,y)}{p(x)p(y)} \right) \\
&= \sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(x)} \right) + p(x,y) \log_2 \left(\frac{p(x,y)}{p(y)} \right) \\
&= \left[\sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(x)} \right) \right] + \left[\sum_x \sum_y p(x,y) \log_2 \left(\frac{p(x,y)}{p(y)} \right) \right] \\
&= \left[\sum_x \underbrace{\left[\sum_x p(x,y) \right]}_{p(x)} \log_2 \left(\frac{1}{p(y)} \right) \right] + \left[\sum_x \sum_y p(x,y) \log_2 \left(p(x|y) \right) \right] \\
&= H(X) - \sum_x \sum_y p(x,y) \log_2 \left(\frac{1}{p(x|y)} \right) \\
&= H(X) - H(X|Y)
\end{aligned}$$

2.2 Entropy of a Continuous Gaussian Random Variable

Show that the entropy $h(X)$ of a continuous Gaussian random variable X is given by

$$h(X) = \frac{1}{2} \log_2(2\pi e \sigma_X^2).$$

Solution:

The Gaussian random variable has the following probability density function (PDF).

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp - \frac{(x-\mu)^2}{2\sigma^2}$$

With this PDF, the entropy yields

$$\begin{aligned}
h(X) &= \int_{-\infty}^{\infty} f_X(x) \log_2 \frac{1}{f_X(x)} \mathrm{dx} \\
&= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(- \frac{(x-\mu)^2}{2\sigma^2} \right) \log_2 \left(\sqrt{2\pi\sigma^2} \exp \left(+ \frac{(x-\mu)^2}{2\sigma^2} \right) \right) \mathrm{dx} \\
&= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(- \frac{(x-\mu)^2}{2\sigma^2} \right) \left[\frac{1}{2} \log_2(2\pi\sigma^2) + \log_2(e) \frac{(x-\mu)^2}{2\sigma^2} \right] \mathrm{dx} \\
&= \frac{1}{2} \log_2(2\pi\sigma^2) \underbrace{\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(- \frac{(x-\mu)^2}{2\sigma^2} \right) \mathrm{dx}}_{1} + \frac{\log_2(e)}{2\sigma^2} \underbrace{\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(- \frac{(x-\mu)^2}{2\sigma^2} \right) (x-\mu)^2 \mathrm{dx}}_{\sigma^2} \\
&= \frac{1}{2} \log_2(2\pi\sigma^2) + \frac{1}{2} \log_2(e) = \frac{1}{2} \log_2(2\pi e \sigma^2)
\end{aligned}$$

Note that the entropy h(X) is independent of the expectation value $E\{X\} = \mu_X$.

2.3 Chain Rules of Entropy and Mutual Information

Chain rules play an important role in information theory.

a) Proof the chain rule of entropy, i.e.

$$H(X_1, X_2, ..., X_N) = \sum_{i=1}^{N} H(X_i|X_{i-1}, ..., X_1).$$

Solution:

$$H(X_1, X_2, ..., X_N) = -\sum_{x_1} \cdots \sum_{x_N} p(x_1, ..., x_N) \log_2 p(x_1, ..., x_N)$$

According to the chain rule for two random variables

$$p(x_1, x_2) = p(x_2|x_1)p(x_1)$$

and its extension to three random variables

$$p(x_1, x_2, x_3) = p(x_3|x_1, x_2)p(x_1, x_2),$$

the joint distribution of N variables can be written as

$$p(x_1, ..., x_N) = \prod_{i=1}^{N} p(x_i|x_{i-1}, ..., x_1)$$

with

$$p(x_i|x_{i-1}, ..., x_1) = p(x_1) \quad \text{for i=1}$$

Thus, the entropy yields

$$\begin{aligned}
H(X_1, X_2, ..., X_N) &= -\sum_{x_1} \cdots \sum_{x_N} p(x_1, ..., x_N) \log_2 \prod_{i=1}^{N} p(x_i|x_{i-1}, ..., x_1) \\
&= -\sum_{x_1} \cdots \sum_{x_N} p(x_1, ..., x_N) \sum_{i=1}^{N} \log_2 p(x_i|x_{i-1}, ..., x_1) \\
&= -\sum_{i=1}^{N} \sum_{x_1} \cdots \sum_{x_N} p(x_1, ..., x_N) \log_2 p(x_i|x_{i-1}, ..., x_1) \\
&= -\sum_{i=1}^{N} \sum_{x_1} \cdots \sum_{x_i} \log_2 p(x_i|x_{i-1}, ..., x_1) \underbrace{\sum_{x_{i+1}} \cdots \sum_{x_N} p(x_1, ..., x_N)}_{p(x_1, ..., x_i)} \\
&= -\sum_{i=1}^{N} \underbrace{\sum_{x_1} \cdots \sum_{x_i} p(x_1, ..., x_i) \log_2 p(x_i|x_{i-1}, ..., x_1)}_{H(X_i|X_{i-1}, ..., X_1)}.
\end{aligned}$$

b) Proof the chain rule for mutual information, i.e.

$$I(X_1, X_2, ..., X_N; Y) = \sum_{i=1}^{N} I(X_i; Y | X_{i-1}, ..., X_1).$$

Solution:

Note that the commas and the semicolon in the notation $I(X_1, ..., X_N; Y)$! The notation clarifies that we compute the mutual information of the random vector $\mathbf{X} = [X_1, ..., X_N]^T$ shared with the random variable Y.

We make use of the following property of the expectation, where $f(\,\cdot\,)$ is a function of the random variable $X_1, ..., X_i$ (e.g. $f(\,\cdot\,) = \log(\,\cdot\,)$):

$$\begin{aligned} E\left\{f(x_1, ..., x_i)\right\} &= \sum_{x_1}\sum_{x_2}\cdots\sum_{x_i} p(x_1, ..., x_i) f(x_1, ..., x_i) \\ &= \sum_{x_1}\cdots\sum_{x_i}\sum_{x_{i+1}}\cdots\sum_{x_N} p(x_1, ..., x_N) f(x_1, ..., x_i) \end{aligned}$$

since we can further reformulate

$$= \sum_{x_1}\cdots\sum_{x_i} f(x_1, ..., x_i) \underbrace{\sum_{x_{i+1}}\cdots\sum_{x_N} p(x_1, ..., x_N)}_{p(x_1, ..., x_i)}$$

Therefore, we can write:

$$\begin{aligned} I(X_1; Y) + I(X_2; Y | X_1) &= E\left\{\log_2 \frac{p(x_1, y)}{p(x_1)p(y)}\right\} + E\left\{\log_2 \frac{p(x_2, y|x_1)}{p(x_2|x_1)p(y|x_1)}\right\} \\ &= \sum_{x_1}\sum_{y} p(x_1, y) \log_2 \frac{p(x_1, y)}{p(x_1)p(y)} \\ &\quad + \sum_{x_1}\sum_{x_2}\sum_{y} p(x_1, x_2, y) \log_2 \frac{p(x_2, y|x_1)}{p(x_2|x_1)p(y|x_1)} \\ &= \sum_{x_1}\sum_{x_2}\sum_{y} p(x_1, x_2, y) \left[\log_2 \frac{p(x_1, y)}{p(x_1)p(y)} \cdot \frac{p(x_2, y|x_1)}{p(x_2|x_1)p(y|x_1)}\right] \\ &= E\left\{\log_2 \frac{p(x_1, y)}{p(x_1)p(y)} \cdot \frac{p(x_2, y|x_1)}{p(x_2|x_1)p(y|x_1)}\right\} \end{aligned}$$

We further investigate the terms, which are given above:

$$\begin{aligned} I(X_1; Y) &= E\left\{\log_2 \frac{p(x_1, y)}{p(x_1)p(y)}\right\} \\ I(X_2; Y | X_1) &= E\left\{\log_2 \frac{p(x_2, y|x_1)}{p(x_2|x_1)p(y|x_1)} \cdot \frac{p(x_1)}{p(x_1)}\right\} \\ &= E\left\{\log_2 \frac{p(x_1, x_2, y)}{p(x_2|x_1)p(x_1, y)}\right\} \\ &\vdots \\ I(X_i; Y | X_1, ..., X_{i-1}) &= E\left\{\log_2 \frac{p(x_i, y|x_1, ..., x_{i-1})}{p(x_i|x_1, ..., x_{i-1})p(y|x_1, ..., x_{i-1})} \cdot \frac{p(x_1, ..., x_{i-1})}{p(x_1, ..., x_{i-1})}\right\} \\ &= E\left\{\log_2 \frac{p(x_1, ..., x_i, y)}{p(x_i|x_1, ..., x_{i-1})p(x_1, ..., x_{i-1}, y)}\right\} \end{aligned}$$

Note: The numerator in $I(X_{i-1}; Y|X_1, ..., X_{i-2})$ and the denominator in $I(X_i; Y|X_1, ..., X_{i-1})$ contain the same term $p(x_1, ..., x_{i-1}, y)$. These terms cancel out in the following sum:

$$\begin{aligned}
\sum_{i=1}^{N} I(X_i; Y|X_1, ..., X_{i-1}) &= E\{\log_2 \frac{p(x_1, y)}{p(x_1)p(y)} \frac{p(x_1, x_2, y)}{p(x_1, y)p(x_2|x_1)} \cdot \cdots \\
&\quad \frac{p(x_1, ..., x_{i-1}, y)}{p(x_1, ..., x_{i-2}, y)p(x_{i-1}|x_1, ..., x_{i-2})} \frac{p(x_1, ..., x_i, y)}{p(x_1, ..., x_{i-1}, y)p(x_i|x_1, ..., x_{i-1})} \cdot \cdots \\
&\quad \frac{p(x_1, ..., x_N, y)}{p(x_1, ..., x_{N-1}, y)p(x_N|x_1, ..., x_{N-1})}\} \\
&= E\left\{\log_2 \frac{p(x_1, ..., x_N, y)}{p(y)\prod_{i=1}^{N} p(x_i|x_1, ..., x_{i-1})}\right\} \\
&= E\left\{\log_2 \frac{p(x_1, ..., x_N, y)}{p(y)p(x_1, ..., x_N)}\right\} \\
&= I(X_1, ..., X_N; Y)
\end{aligned}$$

2.4 Maximum Entropy

In this problem, we will prove, that the entropy of a discrete random variable X with N different realizations x and probability distribution $p(x)$ is upper bounded by

$$H(X) \leq \log_2 N$$

We will make use of the relative entropy (also called the Kullback Leibler divergence)

$$0 \leq D(p||q) = \sum_x p(x) \log_2 \frac{p(x)}{q(x)},$$

which is a measure for the distance of two probability distributions $p(x)$ and $q(x)$. The relative entropy $D(p||q)$ is always non-negative.

a) Determine the probability distribution $q(x)$ of a uniformly distributed random variable X, which can take N different realizations x.

Solution:

The probability distribution of a discrete random variable with N realizations is given as

$$q(x) = \frac{1}{N}$$

b) Determine the entropy $H_u(X)$ of a uniformly distributed random variable X, which can take N different realizations x.

Solution:

The entropy is defined as

$$H(X) = \sum_x p(x) \log_2 \frac{1}{p(x)} = -\sum_x p(x) \log_2 p(x).$$

For the uniformly distributed random variable the entropy is

$$\begin{aligned} H_u(X) &= \sum_x q(x) \log_2 \frac{1}{q(x)} \\ &= \sum_x \frac{1}{N} \log_2 N \\ &= N \frac{1}{N} \log_2 N \\ &= \log_2 N. \end{aligned}$$

c) Determine the relative entropy $D(p||q)$ between a probability distribution $p(x)$ and a uniform probability distribution $q(x)$ depending on the entropy $H(X)$ of a random variable with probability distribution $p(x)$.

Solution:

As given in the task

$$\begin{aligned} D(p||q) &= \sum_x p(x) \log_2 \frac{p(x)}{q(x)} \\ &= \sum_x p(x) \left(\log_2 p(x) + \log_2 \frac{1}{q(x)} \right). \end{aligned}$$

Using the results from above yields

$$\begin{aligned} D(p||q) &= \sum_x p(x) \log_2 p(x) + \sum_x p(x) \log_2 N \\ &= \sum_x p(x) \log_2 p(x) + \log_2 N \sum_x p(x) \\ &= -H(X) + \log_2 N \\ &= \log_2 N - H(X). \end{aligned}$$

d) Use the result from c) in order to prove that $H(X) \leq \log_2 N$.

Solution:

As the relative entropy is non-negative, we know that

$$D(p||q) \geq 0$$

Using the results from above yields

$$\begin{aligned} \log_2 N - H(X) &\geq 0 \\ \log_2 N &\geq H(X). \end{aligned}$$

e) Which probability distribution delivers the maximum possible entropy of a random variable X with N different realizations?

Solution:

From task d) we know that the entropy of the discrete random variable X with N realizations is upper bounded by $\log_2 N$. Task b) showed that this maximum entropy is achieved by the uniform distribution i.e.

$$H_u(X) = \max H(X) = \log_2 N$$

2.5 Conditional Entropy

Show, that $H(X|Y) = 0$ holds for the conditional entropy $H(X|Y)$, if the random variable X is a function of the random variable Y.

Help: $0 \cdot \log_2 0 = 0$ (for convention, since $x \cdot \log_2 x \to 0$ for $x \to 0$).

Solution:

By definition

$$\begin{aligned} H(X|Y) &= \sum_x \sum_y p(x,y) \log_2 \frac{1}{p(x|y)} \\ &= \sum_x \sum_y p(x|y)p(y) \log_2 \frac{1}{p(x|y)} \\ &= \sum_y p(y) \left(\sum_x p(x|y) \log_2 \frac{1}{p(x|y)} \right) \end{aligned}$$

If the random variable X is a function of the random variable Y, then

$$p(x|y) = \begin{cases} 1 & \text{for } x = f(y) \\ 0 & \text{otherwise} \end{cases} .$$

Thus, the summation inside the brackets will result in only two distinct terms, which are either $1 \cdot \log_2 1$ or $0 \cdot \log_2 0$:

$$H(X|Y) = \sum_y p(y) \left(1 \cdot \log_2 1 + 1 \cdot \log_2 1 + 1 \cdot \log_2 1 \ldots 0 \cdot \log_2 0 + 0 \cdot \log_2 0\right).$$

It is easy to see that the term $1 \cdot \log_2 1$ yields 0. According to the hint, the second term $0 \cdot \log_2 0$ yields also 0. As a reminder, the rule of l'Hôspital can be applied to proof that the second term is zero:

$$\lim_{x \to 0} x \log_2 x = \lim_{x \to 0} \frac{\log_2 x}{x^{-1}} = \lim_{x \to 0} \frac{\frac{1}{\ln(2)x}}{-x^{-2}} = \lim_{x \to 0} -\frac{1}{\ln(2)} x = 0 \tag{2.1}$$

Thus, using the the hints from above, we have shown that the entropy is

$$H(X|Y) = \sum_y p(y) \cdot 0 = 0.$$

Chapter 3

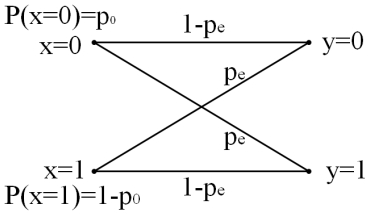
Channel Models and Channel Capacity

3.1 Capacity of the Binary Symmetrical Channel (BSC)

Determine the channel capacity for a binary symmetrical channel (BSC) using the general equation for the mutual information $I(X;Y)$. The transmit symbols from the binary alphabet $x \in \{0,1\}$ have the probabilities

$$P(x) = \begin{cases} p_0 & \text{if} \quad x = 0 \\ 1 - p_0 & \text{if} \quad x = 1 \end{cases}$$

The error probability of the BSC is denoted by p_e.



a) Determine the probabilities $P(y)$ of the output symbols $y = 0$ and $y = 1$.

Solution:
We receive $y = 0$ in the case that the input was $x = 0$ and no error occurred or the input was $x = 1$ and an error occurred. We receive $y = 1$ in the case that the input was $x = 1$ and no error occurred or the input was $x = 0$ and an error occurred.

$$P(y = 0) = (1 - p_e)p_0 \ + \ p_e(1 - p_0) = p_0 - p_e p_0 + p_e - p_0 p_e = p_0 + p_e - 2p_0 p_e$$
$$P(y = 1) = p_e p_0 \ + \ (1 - p_e)(1 - p_0) = p_e p_0 + 1 - p_e - p_0 + p_0 p_e = 1 - (p_0 + p_e - 2p_0 p_e)$$

b) Divide the equation for the mutual information $I(X;Y)$ into two parts such that the first part depends only on the probability $P(y)$ of the channel output symbols y.

Solution:

$$
\begin{aligned}
I(X;Y) &= \sum_{j=1}^{M}\sum_{i=1}^{L} p(x_i,y_j)\log_2\frac{p(x_i;y_j)}{p(x_i)p(y_j)} \\
&= \sum_{j=1}^{M}\sum_{i=1}^{L}\left[p(x_i,y_j)\log_2\frac{1}{p(y_j)} + p(x_i;y_j)\log_2\frac{p(x_i,y_j)}{p(x_i)}\right] \\
&= \left[\sum_{j=1}^{M}\underbrace{\left[\sum_{i=1}^{L}p(x_i,y_j)\right]}_{=p(y_j)}\log_2\frac{1}{p(y_j)}\right] + \left[\sum_{j=1}^{M}\sum_{i=1}^{L}p(x_i,y_j)\log_2 p(y_j|x_i)\right] \\
&= H(Y) - \sum_{j=1}^{M}\sum_{i=1}^{L}p(x_i,y_j)\log_2\frac{1}{p(y_j|x_i)} \\
&= H(Y) - H(Y|X)
\end{aligned}
$$

c) Determine the first term (entropy $H(Y)$) from b) as a function of p_0.

Solution:

$$
\begin{aligned}
H(Y) &= P(y=0)\log_2\left(\frac{1}{P(y=0)}\right) \;+\; (1-P(y=0))\log_2\left(\frac{1}{1-P(y=0)}\right) \\
&= (p_0+p_e-2p_0p_e)\log_2\frac{1}{p_0+p_e-2p_0p_e} \\
&\quad + [1-(p_0+p_e-2p_0p_e)]\log_2\frac{1}{1-(p_0+p_e-2p_0p_e)}
\end{aligned}
$$

d) Determine the second term (conditional entropy $H(Y|X)$) for the given probability distribution $P(x)$ and the given channel transition probabilities $P(y|x)$ depending on p_0 and p_e.

Solution:

$$
\begin{aligned}
H(Y|X) &= -\sum_{j=1}^{M}\sum_{i=1}^{L}p(x_i,y_j)\log_2 p(y_j|x_i) \\
&= -\sum_{j=1}^{M}\sum_{i=1}^{L}p(y_j|x_i)p(x_i)\log_2 p(y_j|x_i) \\
&= -(1-p_e)p_0\log_2(1-p_e) - p_ep_0\log_2(p_e) \\
&\quad -(1-p_e)(1-p_0)\log_2(1-p_e) - p_e(1-p_0)\log_2(p_e) \\
&= -\left[(p_0-p_ep_0+1-p_e-p_0+p_ep_0)\log_2(1-p_e) + (p_ep_0+p_e-p_ep_0)\log_2(p_e)\right] \\
&= -(1-p_e)\log_2(1-p_e) - p_e\log_2(p_e)
\end{aligned}
$$

e) Derive an expression for the mutual information $I(X;Y)$ depending on p_0 and p_e.

Solution:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= (p_0 + p_e - 2p_0p_e)\log_2 \frac{1}{p_0 + p_e - 2p_ep_0} \\ &\quad + (1 - p_0 - p_e + 2p_ep_0)\log_2 \frac{1}{1 - p_0 - p_e + 2p_ep_0} \\ &\quad + (1 - p_e)\log_2(1 - p_e) + p_e \log_2(p_e) \end{aligned}$$

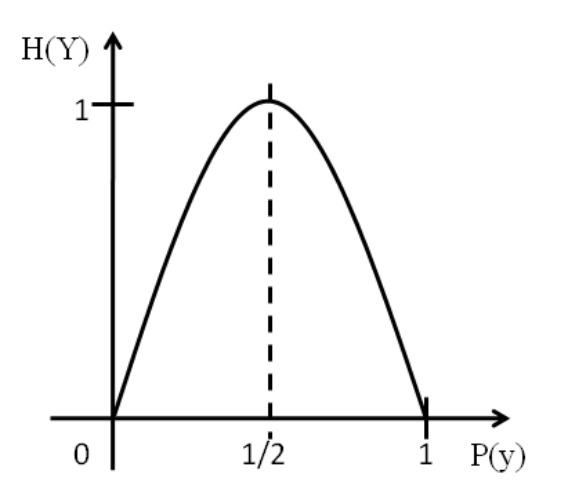
f) Show that the mutual information is maximized for equally likely channel input symbols x.

Solution:

$$I(X;Y) = H(Y) - H(Y|X)$$

As $H(Y|X)$ depends only on p_e it is sufficient to maximize $H(Y)$. Since Y is a binary random variable, $H(Y)$ is given by the binary entropy function

$$H(Y) = H_b(p(y=0)) = H_b(p(y=1) \tag{3.1}$$



$H(Y)$ is maximized if both output symbols $y = 0$ and $y = 1$ occur with the same probability.

As shown in the figure above $H(Y) = 1\,{}^{\text{bit}}/_{\text{channel use}}$ for $P(y=0) = P(y=1) = \frac{1}{2}$.

From a), we have

$$\begin{aligned} P(y=0) &= (1-p_e)p_0 \;+\; (1-p_0)p_e \\ &= p_0 + p_e - 2p_ep_0 \\ &= p_0(1-2p_e) + p_e \overset{!}{=} \frac{1}{2} \end{aligned}$$

For $p_e \neq \frac{1}{2}$

$$\Rightarrow p_0 = \frac{\frac{1}{2} - p_e}{1 - 2p_e} = \frac{1}{2}\frac{1-2p_e}{1-2p_e} = \frac{1}{2}.$$

If $p_e = \frac{1}{2}$ then $P(y=0) = \frac{1}{2}p_0 + (1-p_0)\frac{1}{2} = \frac{1}{2}$ is independent of p_0 and so is $H(Y)$.

g) Determine the channel capacity C of the BSC depending on the channel error probability p_e.

Solution:

$$C = \max_{p(x)} I(X;Y)$$

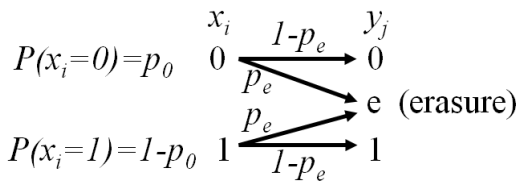
From f) we know that $I(X;Y)$ is maximal for $p(x) = \frac{1}{2}$.

$$\Rightarrow C = 1 + (1-p_e)\log_2(1-p_e) + p_e \log_2(p_e) \qquad = 1 - H_b(p_e),$$

where $H_b(p_e)$ is the binary entropy function.

3.2 Binary Erasure Channel

The binary erasure channel is defined in the following figure:



The transmit symbols x_i are taken from the set $x_i \in \{0,1\}$ with probabilities $P(x_i = 0) = p_0$ and $P(x_i = 1) = 1 - p_0$.
The observed symbols y_j at the channel output are taken from the set $y_i \in \{0,1,e\}$, where 'e' indicates an erasure, i.e. the respective bit is lost.
The channel is symmetric and does not cause corruption of bits. Correct reception of a bit is achieved with probability $1 - p_e$. An erasure occurs with probability p_e.
The channel capacity of the binary erasure channel shall be derived in the following.

a) Determine the probabilities $P(y_j)$ of the channel output symbols y_j depending on p_0 and p_e for all possible realizations of y_j.

Solution:

$$\begin{aligned}
P(y=0) &= p_0(1-p_e) = p_0 - p_0 p_e \\
P(y=e) &= p_0 p_e + (1-p_0)p_e = p_0 p_e + p_e - p_0 p_e = p_e \\
P(y=1) &= (1-p_0)(1-p_e) = 1 - p_0 - p_e + p_o p_e
\end{aligned}$$

b) Determine the entropy $H(Y)$ of the channel output depending on p_0 and p_e. Write $H(Y)$ as a weighted sum of the binary entropy functions $H_b(p_0)$ and $H_b(p_e)$.

Solution:

$$
\begin{aligned}
H(Y) &= \sum_{j=1}^{3} P(y_j) \log_2 \frac{1}{P(y_j)} \\
&= p_0(1-p_e) \log_2 \frac{1}{p_0(1-p_e)} \; + \; p_e \log_2 \frac{1}{p_e} \; + \; (1-p_0)(1-p_e) \log_2 \frac{1}{(1-p_e)(1-p_0)} \\
&= p_0(1-p_e) \left[\log_2 \frac{1}{p_0} + \log_2 \frac{1}{1-p_e} \right] \; + \; p_e \log_2 \frac{1}{p_e} \\
&\quad + (1-p_e) \left[\log_2 \frac{1}{1-p_0} + \log_2 \frac{1}{1-p_e} \right] - p_0(1-p_e) \left[\log_2 \frac{1}{1-p_0} + \log_2 \frac{1}{1-p_e} \right] \\
&\text{which can be sorted for } p_0 \text{ and } p_e \text{ in the } \log_2() \\
&= p_0(1-p_e) \log_2 \frac{1}{p_0} + (1-p_e) \log_2 \frac{1}{1-p_0} - p_0(1-p_e) \log_2 \frac{1}{1-p_0} \\
&\quad + p_0(1-p_e) \log_2 \frac{1}{1-p_e} + p_e \log_2 \frac{1}{p_e} + (1-p_e) \log_2 \frac{1}{1-p_e} - p_0(1-p_e) \log_2 \frac{1}{1-p_e} \\
&= (1-p_e) \underbrace{\left[p_0 \log_2 \frac{1}{p_0} + (1-p_0) \log_2 \frac{1}{1-p_0} \right]}_{H_b(p_0)} + \underbrace{p_e \log_2 \frac{1}{p_e} + (1-p_e) \log_2 \frac{1}{1-p_e}}_{H_b(p_e)} \\
&= (1-p_e) H_b(p_0) + H_b(p_e)
\end{aligned}
$$

c) Determine the probabilities $P(y_j|x_i)$ that y_j is observed given x_i was transmitted for all combinations of realizations x_i and y_j depending on p_0 and p_e.

Solution:

x_i	y_j	$P(y_j\|x_i)$
0	0	$1-p_e$
0	e	p_e
0	1	0
1	0	0
1	e	p_e
1	1	$1-p_e$

d) Determine the joint probabilities $P(x_i, y_j)$ for all combinations of realizations x_i and y_j depending on p_0 and p_e.

Solution:

x_i	y_j	$P(x_i, y_j)$
0	0	$p_0(1-p_e) = p_0 - p_0 p_e$
0	e	$p_0 p_e$
0	1	0
1	0	0
1	e	$(1-p_0)p_e = p_e - p_0 p_e$
1	1	$(1-p_0)(1-p_e) = 1 - p_0 - p_e + p_0 p_e$

e) Determine the mutual information $I(X;Y)$ of channel input and output depending on p_0 and p_e.

Solution:
Help:
Write the expression for $I(X;Y)$ such that the first term is the entropy $H(Y)$ and the second term depends on the binary entropy function $H_b(p_e)$. Then, use the result from task b) in order to simplify the expression.

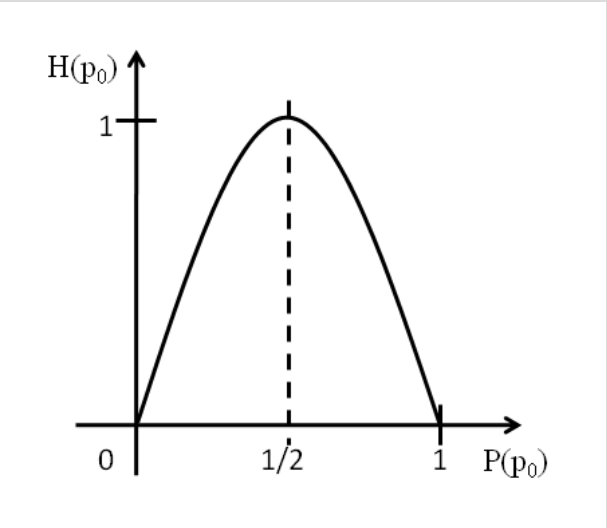
$$
\begin{aligned}
I(X;Y) &= \sum_{i=1}^{2}\sum_{j=1}^{3} P(x_i,y_j)\log_2\frac{P(y_j|x_i)}{P(y_j)} \\
&= \left[\sum_{j=1}^{3}\underbrace{\sum_{i=1}^{2} P(y_j|x_i)P(x_i)}_{P(y_j)}\log_2\frac{1}{P(y_j)}\right] + \left[\sum_{i=1}^{2}\sum_{j=1}^{3} P(x_i,y_j)\log_2 P(y_j|x_i)\right] \\
&= H(Y) \\
&\quad + p_0(1-p_e)\log_2(1-p_e) + p_0 p_e \log_2 p_e \\
&\quad + (1-p_0)p_e\log_2 p_e + (1-p_0)(1-p_e)\log_2(1-p_e) \\
&= H(Y) - p_0 H_b(p_e) - (1-p_0)H_b(p_e) \\
&= H(Y) - H_b(p_e)
\end{aligned}
$$

With $H(Y) = (1-p_e)H_b(p_0) + H_b(p_e)$ from part b) we obtain:

$$
\begin{aligned}
I(X;Y) &= (1-p_e)H_b(p_0) + H_b(p_e) - H_b(p_e) \\
&= (1-p_e)H_b(p_0)
\end{aligned}
$$

f) Determine the input symbol probability p_0 which maximizes the mutual information $I(X;Y)$. Explain your solution clearly.

Solution:
From part e) we know, that $I(X;Y) = (1-p_e)H_b(p_0)$. As p_e is determined by the channel model, the only possibility to maximize $I(X;Y)$ is to maximize $H_b(p_0)$.



$H_b(p_0)$ is maximal for $p_0 = \frac{1}{2}$ and, hence, $I(X;Y)$ maximzed for $p_0 = \frac{1}{2}$.

g) Determine the channel capacity C of the binary erasure channel. Give reasons for your solution.

Solution:
The channel capacity is defined as the maximal achievable mutual information:

$$\begin{aligned} C &= \max_{p_0} I(X;Y) \\ &= \max_{p_0} \{(1-p_e)H_b(p_0)\} \\ &= (1-p_e) \underbrace{\max_{p_0} \{H_b(p_0)\}}_{1} \\ &= 1-p_e \end{aligned}$$

h) Assume that the erasure probability is $p_e = 0.25$. What is the maximum rate R_{max} of an error correcting code which theoretically allows error free transmission through the binary erasure channel? Give reasons for your solution.

Solution:
The channel coding theory requires that $R < C$.

$$\begin{aligned} \Rightarrow R &< 1-p_e \\ R &< 1-0.25 \\ R &< 0.75 \end{aligned}$$

$$\Rightarrow R_{max} = \frac{3}{4}$$

3.3 Capacity of the Binary Input AWGN Channel

Shannon's famous equation

$$C = \frac{1}{2}\log_2\left(1 + \frac{2E_s}{N_0}\right) \tag{3.2}$$

does not put restrictions on the transmit symbol alphabet. The capacity achieving transmit symbol distribution $f_X(x)$ turns out to be a Gaussian distribution. In practice, the transmit symbols can often not be chosen arbitrarily but are determined by the modulation scheme. In case of BPSK modulation, the transmit symbols are taken from the alphabet $X \in \{-1, +1\}$. Such an AWGN channel with binary input is called a *binary-input AWGN channel*.
Show that the capacity of a binary input AWGN channel with input symbols $X \in \{\pm 1\}$ and noise variance σ_N^2 is given by

$$C = -\frac{1}{\sqrt{8\pi\sigma_N^2}}\int_{-\infty}^{\infty}\left(e^{-\frac{(y+1)^2}{2\sigma_N^2}} + e^{-\frac{(y-1)^2}{2\sigma_N^2}}\right)\log_2\left[\frac{1}{\sqrt{8\pi\sigma_N^2}}\left(e^{-\frac{(y+1)^2}{2\sigma_N^2}} + e^{-\frac{(y-1)^2}{2\sigma_N^2}}\right)\right]dy$$
$$-\frac{1}{2}\log_2\left(2\pi e\sigma_N^2\right)$$

Hint: As you saw in previous tasks (binary symmetrical and binary erasure channel) the capacity was obtained for input symbols with equal probability. You can assume that equally probable input symbols do maximize the mutual information for the binary AWGN channel, too.

Solution:

The channel capacity is defined as the maximum mutual information

$$C = \max_{p(x)} I(X;Y)\,,$$

where the maximization is done over the probability distribution $p(x)$ of the channel input symbols X. From Problem 2.1, we know that

$$I(X;Y) = H(Y) - H(Y|X). \tag{3.3}$$

Therefore, we first determine the entropy $H(Y)$ of the channel output and the conditional entropy $H(Y|X)$. Then we maximize over all possible probability distributions $p(x)$. As the channel input X is binary, we only have to find the capacity achieveing probability $P(x = +1) = 1 - P(x = -1)$.

- Let's start with the conditional entropy $H(Y|X)$:

$$\begin{aligned} H(Y|X) &= -\sum_{x\in\{-1,1\}}\int_{-\infty}^{\infty} f_{X,Y}(x,y)\log_2 f_{Y|X}(y|x)dy \\ &= -\sum_{x\in\{-1,1\}} P(x)\int_{-\infty}^{\infty} f_{Y|X}(y|x)\log_2 f_{Y|X}(y|x)dy \end{aligned}$$

  The received symbols are given by $y = x + n$, where n is additive white Gaussian noise with probability density function

$$f_N(n) = \frac{1}{\sqrt{2\pi\sigma_N^2}}e^{-\frac{(n)^2}{2\sigma_N^2}}. \tag{3.4}$$

  Hence, the conditional probability density function $f_{Y|X}(y|x)$ is given by $f_{Y|X}(y|x) = \frac{1}{\sqrt{2\pi\sigma_N^2}}e^{-\frac{(y-x)^2}{2\sigma_N^2}}$. The conditional entropy yields

$$H(Y|X) = -\sum_{x\in\{-1,1\}} P(x) \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y-x)^2}{2\sigma_N^2}} \log_2 \left[\frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y-x)^2}{2\sigma_N^2}} \right] dy.$$

We substitute $n = y - x \;\Rightarrow \frac{dn}{dy} = 1$.

$$\begin{aligned} H(Y|X) &= -\sum_{x\in\{-1,1\}} P(x) \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{n^2}{2\sigma_N^2}} \log_2 \left[\frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{n^2}{2\sigma_N^2}} \right] dn \\ &= -\underbrace{\left[\sum_{x\in\{-1,1\}} P(x) \right]}_{1} \cdot \underbrace{\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{n^2}{2\sigma_N^2}} \log_2 \left[\frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{n^2}{2\sigma_N^2}} \right] dn}_{-h(N) = -\frac{1}{2}\log_2(2\pi e\sigma^2)} \end{aligned}$$

The entropy of a continuous Gaussian random variable $h(N)$ was derived in task 2.2 to be $h(N) = \frac{1}{2}\log_2(2\pi e\sigma^2)$.

$$\Rightarrow \; H(Y|X) = \frac{1}{2}\log_2(2\pi\sigma_N^2 e) \tag{3.5}$$

Note that $H(Y|X)$ is independent of $p(x)$. Therefore, the mutual information is maximized if $p(x)$ is chosen such that $H(Y)$ is maximized.

Maximize H(Y) The entropy $H(Y)$ is computed as follows.

$$\begin{aligned} H(Y) &= \int_{-\infty}^{\infty} f_Y(y) \log_2 \frac{1}{f_Y(y)} dy \\ &= -\int_{-\infty}^{\infty} f_Y(y) \log_2 f_Y(y) dy \end{aligned}$$

The marginal distribution $f_Y(y)$ can be computed using the chain rule by marginalization over X or loosely speaking the variable X is summed out of the joint distribution.

$$f_Y(y) = f_{Y|X}(y|x = +1) \cdot P(x = 1) + f_{Y|X}(y|x = -1) \cdot P(x = -1)$$

Next we make use of the fact that equally probable input symbols maximize the mutual information for a symmetrical channel. Then, the marginal distribution $f_Y(y)$ yields

$$\begin{aligned} f_Y(y) &= \frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y-1)^2}{2\sigma_N^2}} \cdot \frac{1}{2} + \frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y+1)^2}{2\sigma_N^2}} \cdot \frac{1}{2} \\ &= \frac{1}{\sqrt{8\pi\sigma_N^2}} \left(e^{-\frac{(y-1)^2}{2\sigma_N^2}} + e^{-\frac{(y+1)^2}{2\sigma_N^2}} \right). \end{aligned}$$

Substituting the result of the marginal distribution $f_Y(y)$ in the entropy function $H(Y)$, we get

$$H(Y) = \int_{-\infty}^{\infty} -\frac{1}{\sqrt{8\pi\sigma_N^2}} \left(e^{-\frac{(y-1)^2}{2\sigma_N^2}} + e^{-\frac{(y+1)^2}{2\sigma_N^2}} \right) \log_2 \left[\frac{1}{\sqrt{8\pi\sigma_N^2}} \left(e^{-\frac{(y-1)^2}{2\sigma_N^2}} + e^{-\frac{(y+1)^2}{2\sigma_N^2}} \right) \right] dy. \tag{3.6}$$

Plugging (3.5) and (3.6) in (3.3), we obtain

$$C = \max_{p(x)} I(X;Y) = \int_{-\infty}^{\infty} -\frac{1}{\sqrt{8\pi\sigma_N^2}} \left(e^{-\frac{(y-1)^2}{2\sigma_N^2}} + e^{-\frac{(y+1)^2}{2\sigma_N^2}} \right) \log_2 \left[\frac{1}{\sqrt{8\pi\sigma_N^2}} \left(e^{-\frac{(y-1)^2}{2\sigma_N^2}} + e^{-\frac{(y+1)^2}{2\sigma_N^2}} \right) \right] dy - \frac{1}{2} \log_2(2\pi\sigma_N^2 e)$$

3.4 Wireless Transmission

Consider an *AWGN* channel with two-sided noise power spectral density $N_0/2$, bandwidth $B = 5$ MHz and a received signal power P_X of -80 dBm. The receiver is characterized by a noise figure F of 10 dB. The receiver operates at a temperature of 21 °C.

a) Determine the noise power P_N.

Solution:
The noise figure F is defined as the factor, by which the thermal noise power spectral density is enhanced due to imperfections of receiver components. The noise figure is a quality indicator of a receiver.

$$N_0 = F \cdot k \cdot T$$
$$P_N = \frac{N_0}{2} \cdot 2B = N_0 B$$

where k is the Boltzmann constant, $k = 1.38 \cdot 10^{-23}\,\mathrm{Ws/K}$ and T is the temperature in Kelvin.

$$\begin{aligned} 10\log_{10} F = 10\text{ dB} \;\Rightarrow\; F &= 10^{\frac{10}{10}} = 10 \\ T &= 21\,^\circ\mathrm{C} = (21 + 273.15)\text{ K} = 294.15\text{ K} \approx 294\text{ K} \\ N_0 &= [10 \cdot 1.38 \cdot 10^{-23} \cdot 294 WsK/K] = 4.06 \cdot 10^{-20} Ws \\ P_N &= 4.06 \cdot 10^{-20} Ws \cdot 5 \cdot 10^6\text{ Hz} = 2.03 \cdot 10^{-13}\text{ W} \\ &= 10\log_{10}\left(2.03 \cdot 10^{-10}\text{mW}\right) = -96.9\text{ dBm} \end{aligned}$$

b) Determine the signal to noise power ratio (SNR) in dB.

Solution:

$$SNR = \frac{P_X}{P_N}$$

Or this is directly expressed in dB:

$$\begin{aligned} SNR_{dB} = 10\log_{10}\left(\frac{P_X}{P_N}\right) dB &= P_{X,\mathrm{dBm}} - P_{N,\mathrm{dBm}} \\ &= -80\text{ dBm} + 96.9\text{ dBm} \\ &= 16.9\text{ dB} \end{aligned}$$

$$10\log_{10}\frac{P_X}{P_N} = 16.9\text{ dB} \quad \Leftrightarrow\; SNR = 10^{\frac{16.9}{10}} = 48.9$$

c) Determine the theoretically achievable data rate C^* in bit/s, i.e. the data rate which can be transmitted error-free in theory.

Solution

$$C^* = B \cdot \log_2\left(1 + \frac{P_X}{P_N}\right) = 5\text{MHz} \cdot \log_2\left(1 + \frac{10^{-80\text{dBm}}}{10^{-96\text{dBm}}}\right) = 28.26\text{Mbit/s}$$

The connection to the channel capacity $C = 1/2 \log_2\left(1 + \frac{2E_s}{N_0}\right)$ in bit/channel use follows using

- $P_X = \frac{E_s}{T_s}$
- $T_s = \frac{1}{2B}$ (Nyquist rate).
- 1 symbol can be transmitted per time interval T_s, i.e. the channel can be used once per T_s.

$$\begin{aligned} C &= C^* \cdot T_s \\ &= BT_s \log_2\left(1 + \frac{E_s/T_s}{N_0 B}\right) \\ &= \frac{T_s}{2T_s} \log_2\left(1 + \frac{E_s/T_s}{N_0 \cdot 1/2T_s}\right) \\ &= \frac{1}{2} \log_2\left(1 + \frac{2E_s}{N_0}\right) \end{aligned}$$

$$\begin{aligned} C &= C^* \cdot T_s \\ &= BT_s \log_2\left(1 + \frac{E_s/T_s}{N_0 B}\right) \\ &= \frac{T_s}{2T_s} \log_2\left(1 + \frac{E_s/T_s}{N_0 \cdot 1/2T_s}\right) \\ &= \frac{1}{2} \log_2\left(1 + \frac{2E_s}{N_0}\right) \end{aligned}$$

d) What is the capacity-achieving probability distribution $f_X(x)$ of the transmit symbols X?

Solution:

$$C = \max_{P(X)} I(X;Y) = \max_{f_X(x)} \left(H(Y) - H(Y|X)\right)$$

It was derived in problem 3.3 that $H(Y|X)$ is independent of $f_X(x)$. Therefore, it is sufficient to maximize $H(Y)$.

$H(Y)$ is maximal if Y is Gaussian distributed. Since $Y = X + N$, where N is additive white Gaussian noise, Y is Gaussian distributed if X is Gaussian distributed.

$\Rightarrow$ For an *AWGN* channel, the transmit symbols X must be Gaussian distributed with mean $\mu = 0$ and variance $\sigma_X^2 = P_X$ to be capacity achieving.

$$X \sim N(0, P_X)$$

e) Which code rate R and which codeword length N have to be applied for capacity-achieving transmission?

Solution:
The channel coding theorem states that a capacity-achieving code exists, if $R < C$ and $N \to \infty$.

Therefore,

$$R < 2.8\,{}^{\text{bit}}/_{\text{channel use}}$$
$$N \to \infty.$$

Note that each transmit symbol X has to carry information of several information bits.

f) Which data rate could be theoretically achieved if the bandwidth was doubled to $2B$?

Solution:
Suppose $B' = 2B$.

$$P'_N = \frac{N_0}{2} \cdot 2B' = 2P_N = 2 \cdot 2.03 \cdot 10^{-13}\ \text{W} = 4.06 \cdot 10^{-13}\ \text{W}$$

Wider the bandwidth causes more noise power within the passband.

The transmit power remains the same but is distributed over a wider frequency band.

The capacity becomes

$$\begin{aligned} C' &= B' \log_2(1 + \frac{P_X}{P'_N}) \\ &= 10\ \text{MHz} \log_2(1 + \frac{10^{-11}\ \text{W}}{4.06 \cdot 10^{-13}\ \text{W}}) \\ &= 46.7\,{}^{\text{Mbit}}/_{\text{s}} \end{aligned}$$

$$C < C' < 2C \tag{3.7}$$

g) Which transmit power would be required in order to obtain the same achievable data rate as in f) but with the original bandwidth B?

Solution:

$$\begin{aligned} C' &= B \log_2 \left(1 + \frac{P'_X}{P_N}\right) \\ 2^{\frac{C}{B}} &= 1 + \frac{P'_X}{P_N} \\ P'_X &= \left(2^{\frac{C}{B}} - 1\right) P_N \\ &= (2^{\frac{46.7}{5}} - 1) \cdot 2.03 \cdot 10^{-13}\ \text{W} \\ &= 1.3 \cdot 10^{-10}\ \text{W} \end{aligned}$$

in dBm:

$$10 \log_{10} \frac{\text{P}'_\text{X}}{1\ \text{mW}}\ \text{dBm} = 10 \log_{10} \frac{1.3 \cdot 10^{-10}}{10^{-3}}\ \text{dBm} = -69\ \text{dBm}$$

Comparing this with the results of part f) shows

$$\frac{P'_X}{P_X} = \frac{1.3 \cdot 10^{-10}\ \text{W}}{10^{-11}\ \text{W}} = 13.$$

Thus, it is much more efficient to double the bandwidth than to increase the transmit power.

h) Which bandwidth and which transmit power would be required in order to achieve the same data rate as in c) but with uncoded transmission (no channel coding) using *BPSK* modulation at a target bit error probability of 10^{-5}.

Solution:
The data rate in c) was $28\,{}^{\text{Mbit}}/_{\text{s}}$. Using *BPSK* modulation one bit per channel use (per time T_s) is transmitted. The resulting symbol duration is:

$$T_s = \frac{1 \text{ bit}}{28\,{}^{\text{Mbit}}/_{\text{s}}} = \frac{1}{28}\,\mu\text{s}$$

$$\Rightarrow B = \frac{1}{2T_s} = \frac{1}{2}28 \text{ MHz} = 14 \text{ MHz}\,. \text{ (if no excess bandwidth is assumed)}$$

Given the bandwidth B, the noise power can be computed:

$$\begin{aligned} P_N &= \frac{N_0}{2} \cdot 2B = 4.05 \cdot 10^{-20}\,{}^{\text{W}}/_{\text{Hz}} \cdot 14 \cdot 10^6 \text{ Hz} \\ &= 5.7 \cdot 10^{-13} \text{ W}\,. \end{aligned}$$

The bit error probability in the case of *BPSK* is given by

$$P_b = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{E_S}{N_0}}\right)\,.$$

Here it is requested that the bit error probability is smaller than 10^{-5}.

$$\begin{aligned} P_b = \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_S}{N_0}}\right) &\leq 10^{-5} \\ \Leftrightarrow \text{erfc}\left(\sqrt{\frac{E_S}{N_0}}\right) &\leq 2 \cdot 10^{-5} \end{aligned}$$

From an erfc table we obtain:

$$\begin{aligned} \text{erfc}(3.01) &= 2.074 \cdot 10^{-5} \\ \text{erfc}(3.02) &= 1.947 \cdot 10^{-5} \end{aligned}$$

Therefore, $\sqrt{\frac{E_S}{N_0}}$ must be at least 3.02.

$$\Rightarrow \frac{E_S}{N_0} = (3.02)^2 = 9.12$$

Expanding numerator and denominator by $2B = 1/T_s$ yields

$$\begin{aligned} \frac{E_S}{N_0} = \frac{E_S}{N_0} \cdot \frac{2B}{2B} &= \frac{E_s \frac{1}{T_s}}{N_0 B 2} = \frac{P_X}{2P_N} \\ \Rightarrow P_X = \frac{E_S}{N_0} \cdot 2P_N & \\ = 9.12 \cdot 2 \cdot 5.7 \cdot 10^{-13} \text{ W} &= 10.4 \cdot 10^{-12} \text{ W} \end{aligned}$$

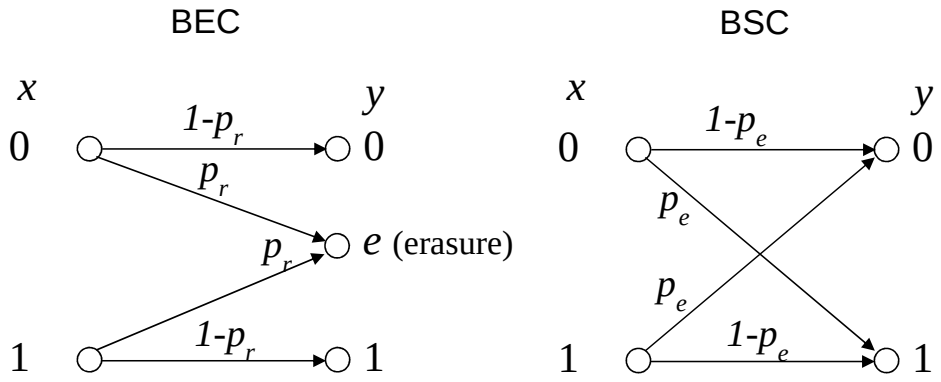
in dBm:

$$10\log_{10}\left(10.4\cdot 10^{-9}\ \text{mW}\right) = -79.8\ \text{dBm}$$

Comparison with c) shows that the transmit power remains almost the same, while the bandwidth is increased by almost a factor of 3.

3.5 BEC vs. BSC

The binary erasure channel (BEC) and the binary symmetrical channel (BSC) should be compared.



The transmit symbols x_i are taken from the set $\{0,1\}$ with probabilities $P(x_i = 0) = p_0$ and $P(x_i = 1) = p_1$. The probability for a transmission error in the BSC is p_e, the probability for an erasure in the BEC is p_r.
The channel capacity of the BSC is

$$C_{\text{BSC}}(p_e) = 1 - H_b(p_e)$$

with the binary entropy function $H_b(p) = -(1-p)log_2(1-p) - p\log_2(p)$.
The mutual information of the BEC is

$$I_{\text{BEC}}(X,Y) = (1-p_r)H_b(p_0)\,.$$

a) Is the BSC a discrete memoryless channel? Why?

Solution:

The BSC is a discrete memoryless channel:

Consider transmission of a sequence of bits $\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. The received values are $\mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$. It holds, that

$$P(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} P(y_i|x_i)\,.$$

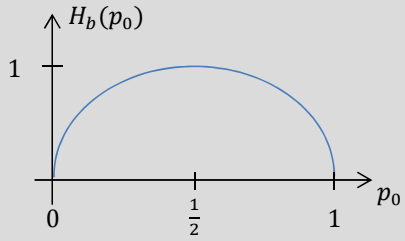
$\Rightarrow$ The channel is memoryless.

b) Which propabilities p_0 and p_1 maximize the mutual information of the BEC?

Solution:

$$I_{\text{BEC}}(X,Y) = \underbrace{(1-p_r)}_{\text{indep. of } p_0,\, p_1} H_b(p_0)$$

Therefore we have to maximize $H_b(p_0)$.



$$\Rightarrow\ p_0 = \frac{1}{2} \text{ maximizes } I_{\text{BEC}}(X,Y)$$
$$\Rightarrow\ p_1 = 1 - p_0 = \frac{1}{2} = p_0$$

c) Determine the channel capacity $C_{\text{BEC}}(p_r)$ of the BEC.

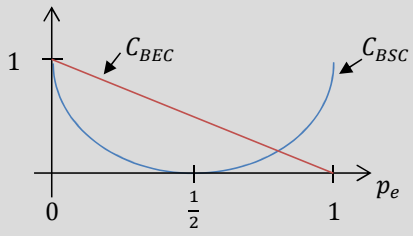
Solution:

$$C_{\text{BEC}} = \max_{p_0} I_{\text{BEC}}(X,Y)$$
$$= (1-p_r)\cdot 1 \,\frac{\text{bit}}{\text{channel use}}$$

d) Show that the channel capacity of the BEC is larger than the one of the BSC for $p_e = p_r < \frac{1}{2}$ (error probability and erasure probability are equal)

Solution:

$$C_{\text{BSC}}(p_e) = 1 - H_b(p_e) \qquad C_{\text{BEC}}(p_r = p_e) = 1 - p_e$$



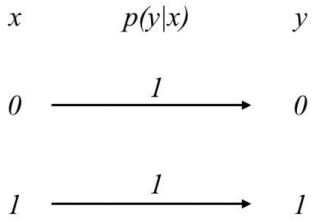
e) Give an vivid explanation of the result from task d)

Solution:

Errors are worse compared to erasures: In the BEC are all received bits correct. The erasures are easily detectable and can be localized. For a given code rate more erasures are correctable than errors.

3.6 Capacity of the Noiseless Binary Channel

The noiseless binary channel is given by the following state transition diagram



a) Determine the channel capacity by intuition. Explain your solution clearly and answer in complete sentences.

Solution:

The channel causes neither errors nor erasures. Each symbol is received correctly. As the channel input is binary, each symbol carries 1 bit hence only 1 bit can be transmitted per channel use. Therefore the channel capacity is 1 bit/channel use.

b) Derive the channel capacity formally. Make sure that all steps in your derivation are clearly given.

Solution:

The channel capacity, C, is given as

$$C = \max_{p(x)} I(X;Y)$$

Where $I(X;Y)$ is the mutual information between the input and output random variables of the channel and $p(x)$ is the probability distribution of the channel input. Then

$$\begin{aligned} I(X;Y) &= \sum_x \sum_y p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \\ &= \sum_x \sum_y p(y|x)p(x) \log_2 \frac{p(y|x)p(x)}{p(x)p(y)} \\ &= \sum_x \sum_y p(y|x)p(x) \log_2 \frac{p(y|x)}{p(y)} \end{aligned}$$

The transition probabilities of the channel can be written as

$$p(y|x) = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases} .$$

The remaining unkown distribtuion is $p(y)$, which can be found by marginalization of the joint distribution $p(x,y)$, i.e.

$$p(y) = \sum_x p(y|x)p(x).$$

Using the transition probability derived above we can compute $p(Y = 0)$ and $p(Y = 1)$.

$$\begin{aligned} p(Y = 0) &= \sum_x p(y|x)p(x) \\ &= P(Y = 0|X = 0)P(X = 0) + P(Y = 0|X = 1)P(X = 1) \\ &= 1 \cdot P(X = 0) + 0 \cdot P(X = 1) \\ &= P(X = 0) \end{aligned}$$

Similarly, it can be shown, that

$$P(Y = 1) = P(X = 1). \tag{3.8}$$

Thus, $p(x) = p(y)$.

The mutual information simplifies into:

$$\begin{aligned} I(X;Y) &= \sum_x p(x) \log_2 \frac{1}{P(Y = x)} \\ &= P(X = 0) \log_2 \frac{1}{P(X = 0)} + P(X = 1) \log_2 \frac{1}{P(X = 1)} \\ &= H_b(P(X = 0)) \end{aligned}$$

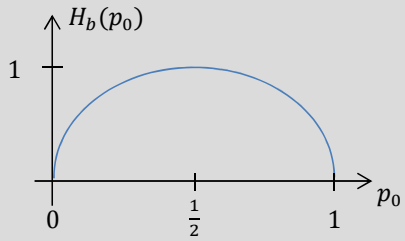
So, the mutual information between the input and output of the channel is a binary entropy function. We know that the maximum value of a binary entropy function is 1. Therefore,

$$C = \max_{p(x)} H_b(P(X = 0)) = 1. \tag{3.9}$$

c) Determine the capacity achieving probability distribution $p(x)$ of the channel input symbols.

Solution:

As seen in task b), the mutual information in this case is a binary entropy function. The maximum value of the binary entropy function is 1 which is attained for $P(X = 0) = 0.5$. This can be seen in the figure below where $P(X = 0)$ is labeled as P_0.

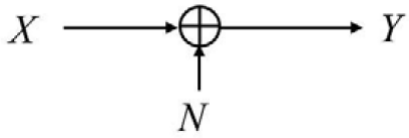


Therefore, the capacity achieving probability distribution is

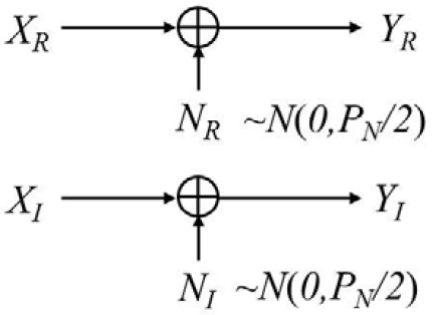
$$P(x = 0) = P(x = 1) = \frac{1}{2}.$$

3.7 Capacity of a Complex AWGN Channel

We consider a discrete-time complex AWGN channel as depicted in the following figure:



The complex noise N is circularly symmetric white and Gaussian with power P_N.The complex AWGN channel could be the equivalent baseband channel of a bandpass transmission scheme. The complex AWGN channel can be represented by two independent real AWGN subchannels (real part and imaginary part) as depicted in the following figure:



The additive white Gaussian noise in real part and imaginary part is uncorrelated, i.e. $E\{N_R \cdot N_I\} = E\{N_R\} \cdot E\{N_I\}$ and has the same power $E\{N_R^2\} = E\{N_I^2\} = \frac{P_N}{2}$.
The total transmit power of the complex AWGN channel is given by P_X.

a) Determine the optimum allocation of the transmit power to the two parallel subchannels (real part and imaginary part).

Solution:

According to the waterfilling principle, the transmit power should be uniformly allocated, i.e.

$$P_R = P_I = \frac{P_X}{2}.$$

b) State the equation for the channel capacity of one of the two subchannels, e.g. for the real part, depending on its input power P_R.

Solution:

Equations for capacity of both real and imaginary subchannels are similar. For the real subchannel, i.e.

$$C_R = 0.5 \log_2 \left(1 + \frac{P_R}{P_N/2}\right).$$

c) Derive the equation for the channel capacity of the complex AWGN channel starting from your result from b).

Solution:

The capacity of a complex channel is sum of the capacities of its real and imaginary subchannels. Therefore,

$$C = C_R + C_I.$$

Using result of subtask b) and a):

$$
\begin{aligned}
C &= 0.5 \log_2 \left(1 + \frac{P_R}{P_N/2}\right) + 0.5 \log_2 \left(1 + \frac{P_I}{P_N/2}\right) \\
&= \log_2 \left(1 + \frac{P_X/2}{P_N/2}\right) \\
&= \log_2 \left(1 + \frac{P_X}{P_N}\right).
\end{aligned}
$$

d) Sketch qualitatively the channel capacity C of the complex AWGN channel vs. the SNR in dB. Label the axes completely.

Solution:

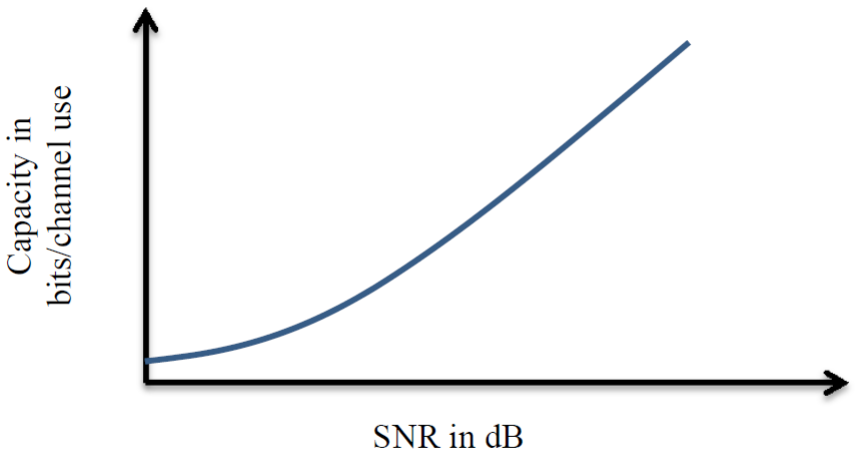


Figure 1: Capacity of a complex AWGN channel with Gaussian input symbols

e) Sketch qualitatively in your plot from d) the capacity CQPSK of the complex AWGN channel, when the transmit symbols are restricted to QPSK.

Solution:

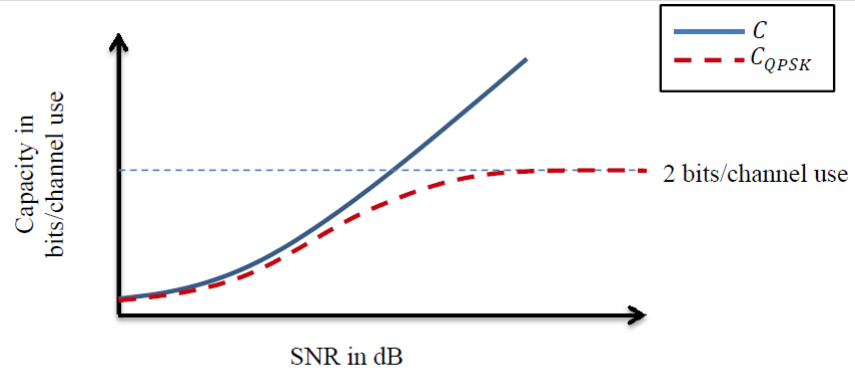


Figure 2: Capacity of a complex AWGN channel with Gaussian input symbols (blue) and QPSK input symbols (red)

f) Discuss, if it makes sense from an information theory point of view to apply QPSK modulation at low SNR or high SNR, respectively.

Solution:

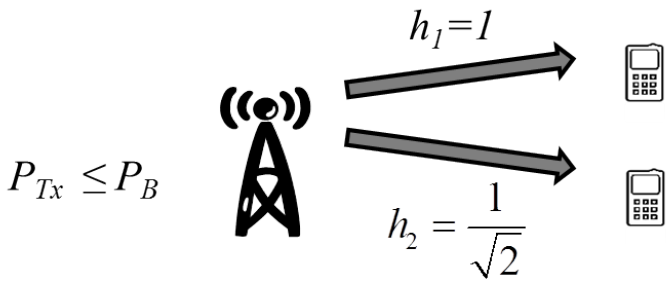
As seen in Figure 2, the gap between the capacity of AWGN channel with optimum input symbols i.e. C, and with QPSK input symbols i.e. C_{QPSK}, is small at low SNR. Therefore, it makes sense to use a lower order modulation scheme such as QPSK at low SNR values. Since QPSK transmits 2 bits per channel use, C_{QPSK} cannot exceed 2 bits/channel use. Therefore, the gap between C and C_{QPSK} becomes large at higher SNR and increasing the SNR does not provide any gain in terms of capacity. Hence QPSK is not suitable at high SNR from information theoretic point of view. Instead, higher order modulation schemes such as 16-QAM, 64-QAM etc are preferable.

Chapter 4

Multi-User Information Theory

4.1 Capacity Region of Downlink TDMA and FDMA in Wireless Communications

Consider the following downlink transmission scenario in a wireless system:



A base station serves two users with independent data. The available bandwidth is $B = 10$ MHz and the maximum transmit power of the base station is $P_B = 10$ W. Each user faces an AWGN channel with noise power spectral density $N_0 = 10^{-20}$ W/Hz in the complex equivalent baseband. The channel coefficients h_k of the two users k, $k \in \{1, 2\}$ are given by

$$h_1 = 1 \qquad h_2 = \frac{1}{\sqrt{2}}$$

The received power at user k is given by $|h_k|^2 P_{\mathbf{Tx}}$, where $P_{\mathbf{Tx}}$ is the transmit power of the base station. The achievable rates with different transmission strategies shall be analyzed in the following problems.

a) Determine the single user capacity C_1 for user 1, i.e. the capacity which is achieved if only user 1 is served.

Solution:

According to Shannon the channel capacity for an AWGN is given by

$$C = B \cdot \log_2 \left(1 + \frac{P_R}{P_N}\right). \tag{4.1}$$

At first we compute the noise power as

$$\begin{aligned} P_N &= \frac{N_0}{2} 2B \\ &= 10^{-20} \text{ W/Hz} \cdot 10 \cdot 10^6 \text{ Hz} \\ &= 10^{-13} \text{ W}. \end{aligned}$$

Thus, the resulting capacity C_1 equals

$$\begin{aligned} C_1 &= B \cdot \log_2\left(1 + \frac{|h_1|^2 P_{\text{Tx}}}{P_N}\right) \\ &= 10 \cdot 10^6 \text{ Hz} \cdot \log_2\left(1 + \frac{1 \cdot 10W}{10^{-13} \text{ W}}\right) \\ &= 465.07 \,\text{Mbit / s}. \end{aligned}$$

b) Determine the single user capacity C_2 for user 2, i.e. the capacity which is achieved if only user 2 is served.

Solution:

According to Shannon the channel capacity for an AWGN is given by

$$C = B \cdot \log_2\left(1 + \frac{P_R}{P_N}\right). \tag{4.2}$$

At first we compute the noise power as

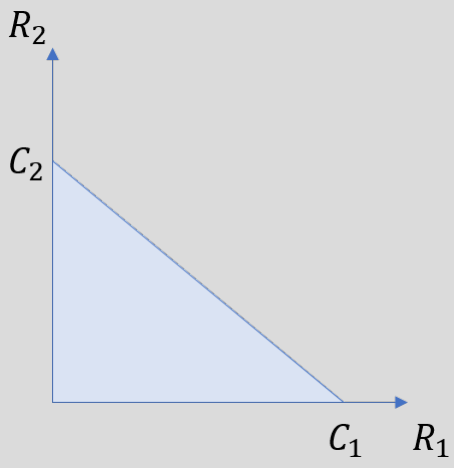
$$\begin{aligned} P_N &= \frac{N_0}{2} 2B \\ &= 10^{-20} \text{ W/Hz} \cdot 10 \cdot 10^6 \text{ Hz} \\ &= 10^{-13} \text{ W}. \end{aligned}$$

Thus, the resulting capacity C_2 equals

$$\begin{aligned} C_2 &= B \cdot \log_2\left(1 + \frac{|h_2|^2 P_{\text{Tx}}}{P_N}\right) \\ &= 10 \cdot 10^6 \text{ Hz} \cdot \log_2\left(1 + \frac{\frac{1}{2} \cdot 10W}{10^{-13} \text{ W}}\right) \\ &= 455.07 \,\text{Mbit / s}. \end{aligned}$$

c) Sketch the achievable rate region for time division multiple access (TDMA) with power constraint.

Solution:



d) Determine the achievable rate pair $R_{1,\text{TDMA}}, R_{2,\text{TDMA}}$ for TDMA, if the channel is allocated to both users for the same fraction of the total transmission time.

Solution:

Since the channel is allocated to both users for the same fraction, each user transmits

half of the time, i.e., $\tau = 0.5$. The achievable rate is then

$$R_{1,\text{TDMA}} = \tau \cdot C_2 = 0.5 \cdot C_1 = 232.53 \text{ Mbit / s}$$
$$R_{2,\text{TDMA}} = \tau \cdot C_2 = 0.5 \cdot C_2 = 227.53 \text{ Mbit / s}$$

e) Determine the achievable rate pair $R_{1,\text{FDMA}}, R_{2,\text{FDMA}}$ for FDMA, if the same fraction of the channel bandwidth is allocated to the two users.

Solution:

Since both users allocate half of the available bandwidth, $B_k = 0.5B, k \in \{1, 2\}$. Similarly, the power assigned to a user needs to be adapted to meet the sum-power constraint of the base station. Consequently, $P_K = 0.5P_{\mathbf{Tx}}, k \in \{1, 2\}$. Due to the reduced bandwidth allocated for user k the noise power changes accordingly, i.e. $P_{N,k} = \frac{N_0}{2} \cdot 0.5 \cdot 2B = 0.5P_N$. The resulting achievable rate pair equals

$$\begin{aligned} R_{k,\text{FDMA}} &= B_k \log_2 \left(1 + \frac{|h_k|^2 P_K}{P_{N,k}}\right) \\ &= 0.5B \log_2 \left(1 + \frac{|h_k|^2 \cdot 0.5P_{\mathbf{Tx}}}{0.5P_N}\right) \\ &= 0.5C_k \end{aligned}$$

Hence,

$$R_{1,\text{FDMA}} = 0.5 \cdot C_1 = 232.53 \text{ Mbit / s}$$
$$R_{2,\text{FDMA}} = 0.5 \cdot C_2 = 227.53 \text{ Mbit / s}$$

f) Determine the achievable sum rate for the TDMA and FDMA schemes in d) and e) where the same fraction of resources for both users is allocated.

Solution:

The achievable sum rate is

$$R_{\text{sum}} = R_1 + R_2 = 0.5C_1 + 0.5C_2$$

for both TDMA with $\tau = 0.5$ and FDMA with $\beta = 0.5$.

g) Which TDMA and FDMA transmission strategy maximizes the sum rate?

Solution:

Since $|h_1| > |h_2|$, the sum rate is maximized, if only user 1 is served.

h) Determine the maximum sum rate according to your solution from g).

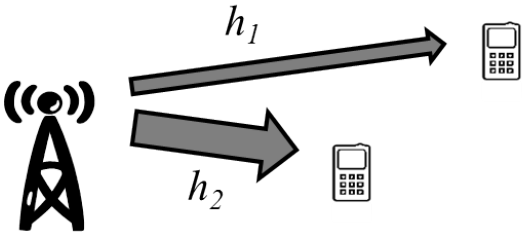
Solution:

The maximum sum rate is achieved, if only the user with the highest rate is served, i.e.,

$$R_{\text{sum,max}} = \max\{R_1, R_2\} = C_1$$

4.2 Capacity Region of Superposition Coding in a Broadcast Channel

Consider a wireless broadcast channel, where a base station serves two users:



The available bandwidth is denoted B and the maximum transmit power of the base station is P_B. The received signal at user k is given by

$$y_k = h_k x + n_k, \tag{4.3}$$

where h_k is the channel coefficient of user k, x is the transmit signal and n_k is additive white Gaussian noise with the same power P_N at both users.
The base station applies superposition coding strategy such that the transmit signal is a superposition of the signals s_k intended for the two users $k \in \{1, 2\}$:

$$x = s_1 + s_2, \tag{4.4}$$

where s_k is contained in x with power P_k and

$$P_1 + P_2 \leq P_B.$$

Under the assumption that

$$|h_1|^2 < |h_2|^2,$$

the achievable rates for the superposition coding strategy have been shown to be given by the following expressions:

$$R_1 = B \log_2 \left(1 + \frac{|h_1|^2 P_1}{|h_1|^2 P_2 + P_N} \right), \tag{4.5}$$

$$R_2 = B \log_2 \left(1 + \frac{|h_2|^2 P_2}{P_N} \right). \tag{4.6}$$

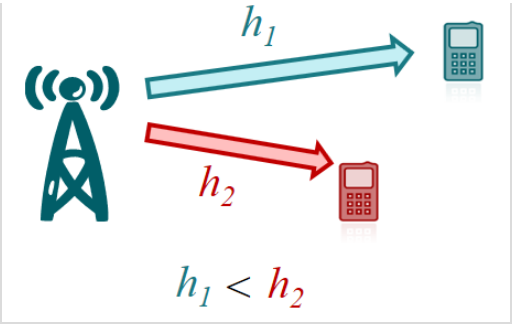
a) Which power allocation P_1, P_2 in equation (4.4) corresponds to a single user transmission?

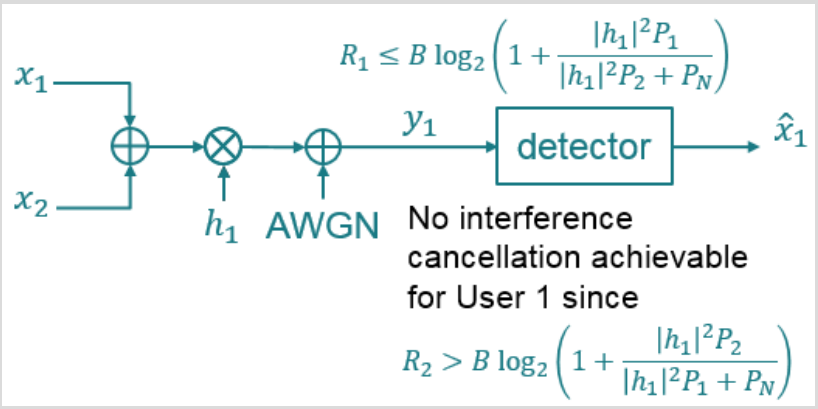
$P_1 \leq P_B, P_2 = 0 \Rightarrow$ only user 1 is served
$P_2 \leq P_B, P_1 = 0 \Rightarrow$ only user 2 is served

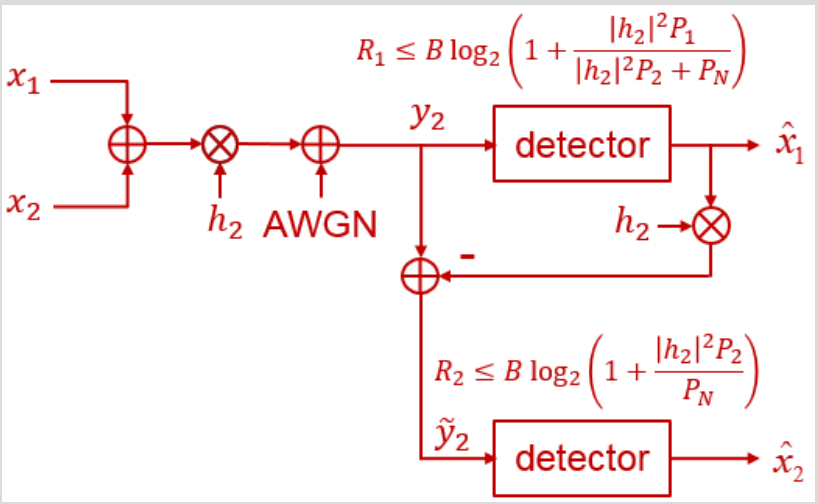
b) Give an interpretation of equations (4.5) and (4.6): Which transmission and detection strategies can achieve the rates according to (4.5) and (4.6)? Answer in complete sentences!

User 2 transmits at its single user capacity. User 1 transmits at a rate which is supported, if the signal of user 2 occurs as additional AWGN.

User 2 experiences the better channel quality. Hence, user 2 can detect for user 1 and subtract it from its received signal. Then, it can detect its own signal as if the signal for user 1 was not present. User 1 experiences the worse channel. It cannot detect the signal for user 2 as the rate of user 2 exceeds the channel capacity of user 1, i.e. $R_2 > C_1$. Hence, user 1 detects its signal while treating the signal for user 2 as additional additive white Gaussian noise (AWGN) with power $|h_1|^2 P_2$. The signal for user 2 can be regarded as independent white Gaussian noise, since the optimum transmit signal in an AWGN channel is Gaussian distributed and consequently, both s_1 and s_2 are Gaussian distributed.







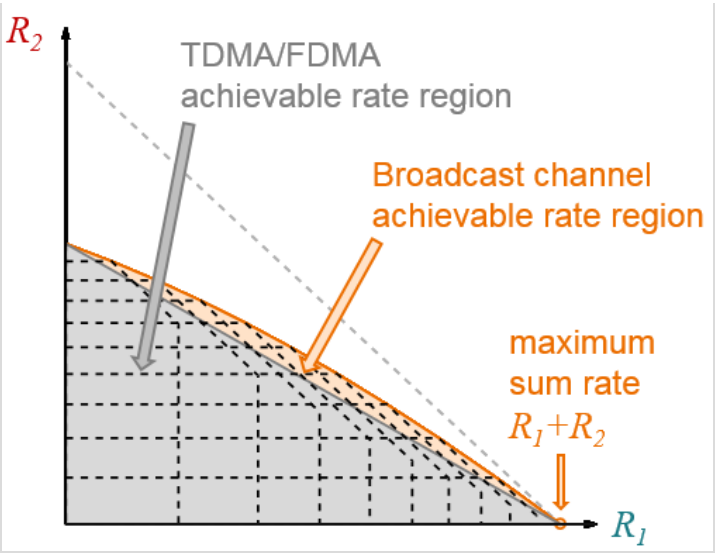
c) Determine an equation for the achievable rate region of superposition coding.

The achievable rate region for a Broadcast channel is equal to the union of all corresponding dual MAC capacity regions.

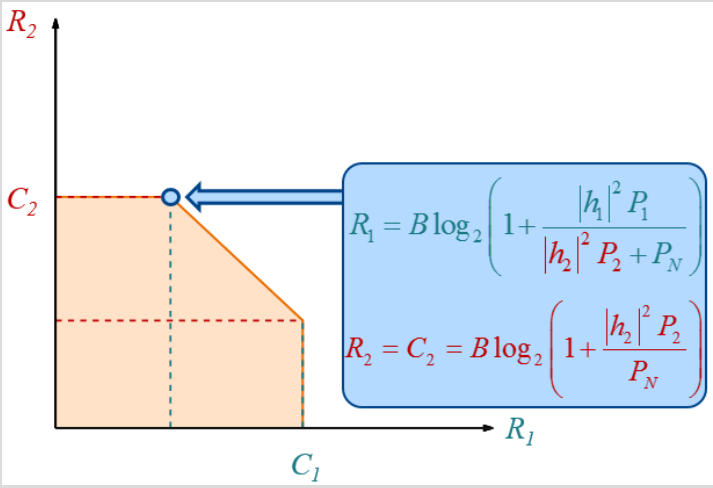
$$C_{SC} = \bigcup_{P_1, P_2 : P_1 + P_2 \leq P_B} C_{\text{dual MAC}}(P_1, P_2)$$

It has been stated in the task description, that the achievable rates R_1 and R_2 for the superposition coding strategy are given by equation 4.5 and 4.6. Further, a detection strategy has been developed in task b) which achieves these rates.

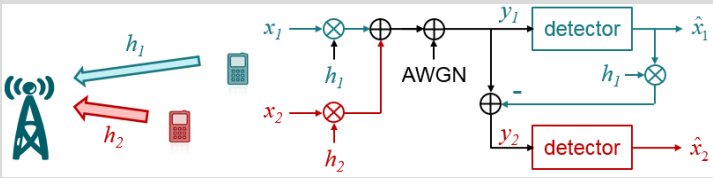
In following figure the union of dual MAC capacity regions (dashed lines) leads to the capacity region of the broadcast channel (solid orange line).



In case of $h_1 < h_2$ the orange line is determined by the connection of upper corners from all dual MAC capacity regions. As an example the subsequent figure shows this corner point.



For a dual MAC the upper corner point of the capacity region can be achieved through interference cancellation techniques. Notice that the resulting rates R_1 and R_2 correspond to the equations 4.5 and 4.6 of the task description, even though the detector for the dual MAC is slightly different compared to broadcast detector of task b).



Thus, we can simply take the union of all rate pairs resulting from combinations of P_1 and P_2 with $P_1 + P_2 \leq P_{\mathrm{BC}}$ to define the achievable rate region as

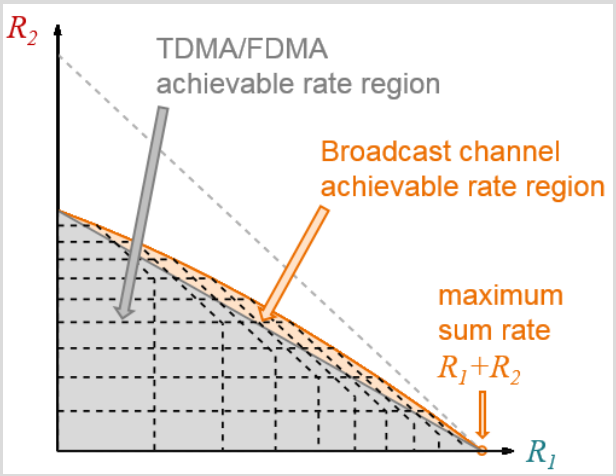
$$C_{SC} = \bigcup_{P_1,P_2:P_1+P_2\leq P_B} \left[R_1 = B\log_2\left(1+\frac{|h_1|^2 P_1}{|h_1|^2 P_2 + P_N}\right), R_2 = B\log_2\left(1+\frac{|h_2|^2 P_2}{P_N}\right)\right]$$

d) Is superposition coding an optimum transmission scheme in the sense that it can achieve the maximum possible rate region? Give clear reasons and answer in complete sentences!

The ultimate rate region which is achievable for a given power constraint without prior restriction of the multiple access scheme is called the capacity region. The rate region in c) is equal to the capacity region of the broadcast channel, since it is the union of the dual MAC capacity regions for all power allocations P_1, P_2. Therefore, superposition coding is an optimum transmission strategy.

e) Which transmission strategy maximizes the sum rate of superposition coding in case of unequal channel quality, i.e. $|h_1|^2 \neq |h_2|^2$?

In case of $|h_1|^2 \neq |h_2|^2$, the sum rate is maximized, if all resources are allocated to the user with the better channel quality. I.e., if $|h_k| > |h_l|$, only user k should be served with $P_k = P_B, P_l = 0$. User k can then transmit at its single user capacity.

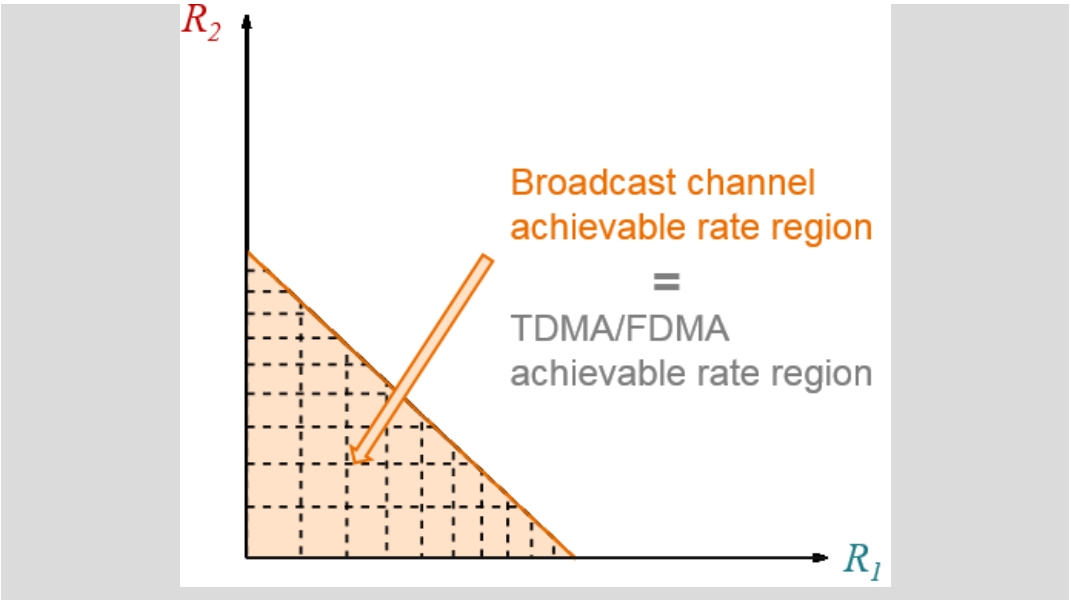


f) Determine an equation for the maximum sum rate according to your solution from e).

$$\max\{R_1 + R_2\} = \max\left\{B\log_2\left(1 + \frac{|h_1|^2 P_B}{P_N}\right), B\log_2\left(1 + \frac{|h_2|^2 P_B}{P_N}\right)\right\}$$

g) Under which condition for $|h_1|^2$ and $|h_2|^2$ does superposition coding provide a larger achievable rate region than time division multiple access (TDMA) ?

For $|h_1| = |h_2|$, the broadcast channel capacity region is equal to the achievable rate region of TDMA. Hence, superposition coding provides a larger achievable rate region than TDMA only if $|h_1| \neq |h_2|$.


R_2
Broadcast channel
achievable rate region
=
TDMA/FDMA
achievable rate region
R_1

Chapter 5

Decoding Principles

5.1 Hard Decision and Soft Decision, Maximum Likelihood (ML) and Maximum A-Posterior (MAP) Decoding

Consider a rate $R = \frac{1}{3}$ repetition code. The information bit sequence $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T$ shall be transmitted. For transmission, we use BPSK modulation, where the mapping of a code bit x_i to a transmit symbol d_i is given by

$$x_i = 0 \longrightarrow d_i = +1$$
$$x_i = 1 \longrightarrow d_i = -1$$

a) Determine the encoded bit sequence $\mathbf{x}$. How many codewords are transmitted?

Solution:

$$\begin{aligned} \mathbf{u} &= \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix}^T \\ &= \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T \\ \mathbf{x} &= \begin{bmatrix} \mathbf{x}_1^T & \mathbf{x}_2^T & \mathbf{x}_3^T \end{bmatrix}^T \\ &= \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^T \end{aligned}$$

b) Determine the sequence $\mathbf{d}$ of BPSK modulated transmit symbols.

Solution:

$$\begin{aligned} \mathbf{x} &= \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^T \\ \mathbf{d} &= \begin{bmatrix} \mathbf{d}_1 & \mathbf{d}_2 & \mathbf{d}_3 \end{bmatrix}^T \\ &= \begin{bmatrix} +1 & +1 & +1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}^T \end{aligned}$$

The BPSK symbols are transmitted through an AWGN channel. The received sequence is given by

$$\mathbf{y} = \begin{bmatrix} +0.3 & -0.1 & +2.0 & +0.1 & +0.2 & -2.0 & +0.1 & +0.2 & -0.2 \end{bmatrix}^T .$$

c) Determine for each information bit the decoding result in case of

1) hard decision maximum likelihood (ML) decoding. Check, if decoding errors occur.

Solution:

The Maxmimum Likelihood (ML) criterion for this example is derived as follows.

$$\begin{aligned}\hat{\mathbf{u}} &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p(\mathbf{y}|\mathbf{d}) \\ &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p([y_1, ..., y_N]^T|[d_1, ..., d_N]^T) \\ &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} \prod_{i=1}^{N} p(y_i|d_i) \\ &\text{(memoryless channel)}\end{aligned}$$

$$\begin{aligned}\hat{\mathbf{u}} &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \frac{-(y_i - d_i)^2}{2\sigma^2} \\ &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} \sum_{i=1}^{N} -(y_i - d_i)^2 \\ &\text{(applying the logarithm to the objective function)} \\ &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmin}} \sum_{i=1}^{N} (y_i - d_i)^2 \\ &\text{(minimizing the negative objective function is equivalent} \\ &\text{to maximizing the objective function)}\end{aligned}$$

For this example the information word $\mathbf{u}$ is vector of length one, i.e. $\mathbf{u} = u_k$. Hard decision maximum-likelihood decoding:

$$\hat{u}_k = \underset{u_k\to\mathbf{d}_k}{\text{argmin}} \sum_{i=1}^{3} (\hat{y}_i - d_i)^2$$

$$\begin{array}{rcccccccccc} \mathbf{y} & = & [& +0.3 & -0.1 & +2.0 & +0.1 & +0.2 & -2.0 & +0.1 & +0.2 & -0.2 &]^T \\ \hat{\mathbf{y}} & = & [& +1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 &]^T \end{array}$$

(Hard decision on received samples $\mathbf{y}$ before decoding)

For $\hat{u}_1 = 0 \longrightarrow d_i = +1$:

$$\begin{aligned}\sum_{i=1}^{3} (\hat{y}_i - 1)^2 &= (+1-1)^2 + (-1-1)^2 + (+1-1)^2 \\ &= (0)^2 + (-2)^2 + (0)^2 = 4\end{aligned}$$

For $\hat{u}_1 = 1 \longrightarrow d_i = -1$:

$$\begin{aligned}\sum_{i=1}^{3} (\hat{y}_i + 1)^2 &= (+1+1)^2 + (-1+1)^2 + (+1+1)^2 \\ &= (+2)^2 + (0)^2 + (+2)^2 = 8\end{aligned}$$

$$\hat{u}_1 = 0$$

For $\hat{u}_2 = 0 \longrightarrow d_i = +1$:

$$\sum_{i=1}^{3}(\hat{y}_i - 1)^2 = (+1-1)^2 + (+1-1)^2 + (-1-1)^2$$
$$= (0)^2 + (0)^2 + (-2)^2 = 4$$

For $\hat{u}_2 = 1 \longrightarrow d_i = -1$:

$$\sum_{i=1}^{3}(\hat{y}_i + 1)^2 = (+1+1)^2 + (+1+1)^2 + (-1+1)^2$$
$$= (+2)^2 + (+2)^2 + (0)^2 = 8$$

$$\hat{u}_2 = 0$$

For $\hat{u}_3 = 0 \longrightarrow d_i = +1$:

$$\sum_{i=1}^{3}(\hat{y}_i - 1)^2 = (+1-1)^2 + (+1-1)^2 + (-1-1)^2$$
$$= (0)^2 + (0)^2 + (-2)^2 = 4$$

For $\hat{u}_3 = 1 \longrightarrow d_i = -1$:

$$\sum_{i=1}^{3}(\hat{y}_i + 1)^2 = (+1+1)^2 + (+1+1)^2 + (-1+1)^2$$
$$= (+2)^2 + (+2)^2 + (0)^2 = 8$$

$$\hat{\mathbf{u}} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

In comparison with $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T$, two bit errors occurred.

2) soft decision maximum likelihood (ML) decoding. Check, if decoding errors occur.

Solution:

Soft decision maximum-likelihood decoding:

$$\hat{u}_k = \underset{u_k \to \mathbf{d}}{\operatorname{argmin}} \sum_{i=1}^{3}(y_i - d_i)^2$$

For $\hat{u}_1 = 0 \longrightarrow d_i = +1$:

$$\sum_{i=1}^{3}(y_i - 1)^2 = (+0.3-1)^2 + (-0.1-1)^2 + (+2.0-1)^2$$
$$= (-0.7)^2 + (-1.1)^2 + (+1.0)^2 = 2.7$$

For $\hat{u}_1 = 1 \longrightarrow d_i = -1$:

$$\sum_{i=1}^{3}(y_i + 1)^2 = (+0.3+1)^2 + (-0.1+1)^2 + (+2.0+1)^2$$
$$= (+1.3)^2 + (+0.9)^2 + (+3.0)^2 = 11.5$$

$$\hat{u}_1 = 0$$

For $\hat{u}_2 = 0 \longrightarrow d_i = +1$:

$$\sum_{i=1}^{3}(y_i - 1)^2 = (+0.1 - 1)^2 + (+0.2 - 1)^2 + (-2.0 - 1)^2$$
$$= (-0.9)^2 + (-0.8)^2 + (-3.0)^2 = 10.45$$

For $\hat{u}_2 = 1 \longrightarrow d_i = -1$:

$$\sum_{i=1}^{3}(y_i + 1)^2 = (+0.1 + 1)^2 + (+0.2 + 1)^2 + (-2.0 + 1)^2$$
$$= (+1.1)^2 + (+1.2)^2 + (-1.0)^2 = 3.65$$

$$\hat{u}_2 = 1$$

For $\hat{u}_3 = 0 \longrightarrow d_i = +1$:

$$\sum_{i=1}^{3}(y_i - 1)^2 = (+0.1 - 1)^2 + (+0.2 - 1)^2 + (-0.2 - 1)^2$$
$$= (-0.9)^2 + (-0.8)^2 + (-1.2)^2 = 2.89$$

For $\hat{u}_3 = 1 \longrightarrow d_i = -1$:

$$\sum_{i=1}^{3}(y_i + 1)^2 = (+0.1 + 1)^2 + (+0.2 + 1)^2 + (-0.2 + 1)^2$$
$$= (+1.1)^2 + (+1.2)^2 + (-0.8)^2 = 3.29$$

$$\hat{\mathbf{u}} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

In comparison with $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T$, one bit error occurred. Note that with soft decision decoding, only one bit error occurs in the decoded information word $\hat{\mathbf{u}}$, while hard decision decoding resulted in two bit errors in the decoding result.

Assume that the source bits $u_k = 0$ and $u_k = 1$ are equally likely, i.e. $P(u_k = 0) = P(u_k = 1) = 0.5$.

d) Determine for each information bit the decoding result in case of

1) hard decision maximum a-posteriori (MAP) dedoding. Check, if decoding errors occur and compare to the result of problem c).

Solution:

The Maxmimum A-Posteriori (MAP) criterion for this example is derived as follows.

$$\begin{aligned}
\hat{\mathbf{u}} &= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p(\mathbf{d}|\mathbf{y}) \\
&= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p(\mathbf{y}|\mathbf{d}) P_a(\mathbf{d}) \\
&= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p(\mathbf{y}|\mathbf{d}) P(\mathbf{u}=\hat{\mathbf{u}}) \\
&= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} p([d_1,...,d_N]^T|[y_1,...,y_N]^T) P_a([u_1,...,u_K]^T) \\
&= \underset{\mathbf{u}\to\mathbf{d}}{\text{argmax}} \prod_{i=1}^{N} p(y_i|d_i) \prod_{k=1}^{K} P_a(u_k) \\
&= \underset{u_k\to\mathbf{d}_k}{\text{argmax}} \left(\prod_{i=1}^{N} p(y_i|d_i) \right) P_a(u_k) \\
&\quad \text{(information word has length } K=1)
\end{aligned}$$

Hard decision maximum a-posteriori decoding:

$$\hat{u}_k = \underset{u_k\to\mathbf{d}}{\text{argmax}} \left(\prod_{i=1}^{3} P(\hat{y}_i|d_i) \right) P_a(u_k)$$

For an AWGN channel with a noise power of σ_N^2, the objective function yields

$$\begin{aligned}
\hat{u_k} &= \underset{u_k\to\mathbf{d}_k}{\text{argmax}} \left(\prod_{i=1}^{3} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \frac{-(y_i-d_i)^2}{2\sigma^2} \right) P_a(u_k) \\
&\quad \text{(applying the logarithm to the objective function)} \\
&= \underset{u_k\to\mathbf{d}_k}{\text{argmax}} \left(\sum_{i=1}^{3} \frac{-(y_i-d_i)^2}{2\sigma^2} \right) + \log(P_a(u_k)) \\
&= \underset{u_k\to\mathbf{d}_k}{\text{argmin}} \left(\sum_{i=1}^{3} \frac{(y_i-d_i)^2}{2\sigma^2} \right) - \log(P_a(u_k)) \\
&\quad \text{(minimizing the negative objective function is equivalent} \\
&\quad \text{to maximizing the objective function)} \\
&= \underset{u_k\to\mathbf{d}_k}{\text{argmin}} \frac{1}{2\sigma_N^2} \left(\sum_{i=1}^{3} (\hat{y}_i-d_i)^2 \right) - \log\left(P_a(u_k)\right)
\end{aligned}$$

with $P_a(u_k=0) = P_a(u_k=1)$

$$\begin{aligned}
&= \underset{u_k\to\mathbf{d}_k}{\text{argmin}} \frac{1}{2\sigma_N^2} \left(\sum_{i=1}^{3} (\hat{y}_i-d_i)^2 \right) \\
&= \underset{u_k\to\mathbf{d}_k}{\text{argmin}} \sum_{i=1}^{3} (\hat{y}_i-d_i)^2
\end{aligned}$$

For equally likely information bits, the MAP and ML criterion yield the same decoding rule. Therefore, we obtain

$$\hat{\mathbf{u}} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

In comparison with $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T$, two bit errors occurred, which is the same as for hard decision ML decoding.

2) soft decision maximum a-posteriori (MAP) decoding. Check, if decoding errors occur and compare to the result of problem c).

Solution:

Soft decision maximum a-posteriori decoding:

$$\hat{u}_k = \underset{u_k \to \mathbf{d}}{\operatorname{argmax}} \left(\prod_{i=1}^{3} P(y_i|d_i) \right) P_a(u_k)$$

for AWGN with power σ_N^2

$$= \underset{u_k \to \mathbf{d}}{\operatorname{argmin}} \frac{1}{2\sigma_N^2} \left(\sum_{i=1}^{3} (y_i - d_i)^2 \right) - \log\left(P_a(u_k)\right)$$

with $P_a(u_k = 0) = P_a(u_k = 1)$

$$= \underset{u_k \to \mathbf{d}}{\operatorname{argmin}} \frac{1}{2\sigma_N^2} \left(\sum_{i=1}^{3} (y_i - d_i)^2 \right)$$
$$= \underset{u_k \to \mathbf{d}}{\operatorname{argmin}} \sum_{i=1}^{3} (y_i - d_i)^2$$

For equally likely information bits, the MAP and ML criterion yield the same decoding rule. Therefore, we obtain

$$\hat{\mathbf{u}} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

In comparison with $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T$, one bit error occurred, which is the same as for soft decision ML decoding.

Assume now that the source emits a bit $u_k = 1$ with higher probability than a bit $u_k = 0$. More precisely, we have $P(u_k = 0) = \frac{1}{4}$ and $P(u_k = 1) = \frac{3}{4}$.

e) Determine for each information bit the decoding result in case of soft decision maximum a-posteriori (MAP) decoding for signal to noise power ratios (SNRs) of 0 dB, 5 dB, 10 dB and 100 dB. Check, if decoding errors occur and compare to the results of problems c) and d).

Solution:

Soft decision maximum a-posteriori decoding:

$$\hat{u}_k = \underset{u_k \to \mathbf{d}}{\operatorname{argmax}} \left(\prod_{i=1}^{3} P(y_i|d_i) \right) P_a(u_k)$$

For an AWGN channel with a noise power of σ_N^2, the objective function yields

$$\hat{u}_k = \underset{u_k \to \mathbf{d}}{\operatorname{argmin}} \underbrace{\frac{1}{2\sigma_N^2} \left(\sum_{i=1}^{3} (y_i - d_i)^2 \right) - \log\left(P_a(u_k)\right)}_{m(\sigma_N^2, y_k, u_k)} \tag{5.1}$$

Note that the noise variance σ_N^2 appears as a weighting factor between channel information and a-priori information $P_a(u_k)$. The stronger the noise power σ_N^2, the more the decoder relies on the a-prior information. The a-prior information denotes the knowledge

of the decoder about the source symbol statistics. For the normalized channel model, the noise variance σ_N^2 is calculated as:

$$\sigma_N^2 = \frac{1}{\text{SNR}},$$

resulting in:

SNR in dB	SNR	σ_N^2
0	1	1
5	$10^{\frac{1}{2}}$	$10^{-\frac{1}{2}}$
10	10	0.1
100	10^{10}	10^{-10}

For the given source symbol statistics

$$-\log\left(P_a(u_k=0)\right) = -\log\left(\frac{1}{4}\right) \approx 1.3863$$
$$-\log\left(P_a(u_k=1)\right) = -\log\left(\frac{3}{4}\right) \approx 0.2877,$$

we can calculate the metric $m(\sigma_N^2, y_k, u_k)$ 5.1 for all possible arguments:

$m(\sigma_N^2, y_k, u_k)$	0 dB	5 dB	10 dB	100 dB
$\hat{u}_1 = 0$	2.7363	5.6554	14.8863	$1.350 \cdot 10^{10} + 1.3863$
$\hat{u}_1 = 1$	6.0377	18.4708	57.7877	$5.750 \cdot 10^{10} + 0.2877$
$\hat{u}_2 = 0$	6.6113	17.9092	53.6363	$5.225 \cdot 10^{10} + 1.3863$
$\hat{u}_2 = 1$	2.1127	6.0588	18.5377	$1.825 \cdot 10^{10} + 0.2877$
$\hat{u}_3 = 0$	2.8313	5.9558	15.8363	$1.445 \cdot 10^{10} + 1.3863$
$\hat{u}_3 = 1$	1.9327	5.4896	16.7377	$1.645 \cdot 10^{10} + 0.2877$

According to 5.1, the MAP decision is the information word $\hat{u}_k$ that minimizes the metric $m(\sigma_N^2, y_k, u_k)$. Thus, we choose the $\hat{u}_k$ with the smallest metric $m(\sigma_N^2, y_k, u_k)$:

	0 dB	5 dB	10 dB	100 dB	*c)/d)*
$\hat{u}_1$	0	0	0	0	0
$\hat{u}_2$	1	1	1	1	1
$\hat{u}_3$	1	1	0	0	0
errors	0	0	1	1	1

For high SNRs, the decoder relies almost only on received samples because the received samples seem to be reliable.

For low SNRs errors can be corrected because of the high impact of a-priori information.

The errors at high SNR are in this example due to the arbitrarily chosen received vector $\mathbf{y}$. Actually at very high SNR, the received vector should almost identical to the transmitted codeword vector.

f) Hard decision decoding can be viewed as receiving data from a binary symmetric channel (BSC) with error probability p_e. Consider hard decision MAP decoding with source statistics $P(u_k = 0) = \frac{1}{4}$ and $P(u_k = 1) = \frac{3}{4}$. Determine the range of channel error probabilities p_e, for which a MAP decoder will decode $\hat{u} = 0$, given that the sequence $\hat{\mathbf{y}} = \begin{bmatrix}+1 & -1 & +1\end{bmatrix}^T$ was received.

Solution:

The channel transition probabilities for a BSC are given by:

$$\begin{aligned}\hat{u} &= \underset{u\to\mathbf{d}}{\operatorname{argmax}} \left(\prod_{i=1}^{3} P(\hat{y}_i|d_i)\right) P_a(u) \\ &= \underset{u\to\mathbf{d}}{\operatorname{argmax}}\ P(+1|d_1)\cdot P(-1|d_2)\cdot P(+1|d_3)\cdot P_a(u)\end{aligned}$$

We distinguish the two cases error free and erroneous:

Error free:

$$\begin{aligned}P(\hat{y}_i = +1|d_i = +1) &= 1-p_e \\ P(\hat{y}_i = -1|d_i = -1) &= 1-p_e\end{aligned}$$

Erroneous:

$$\begin{aligned}P(\hat{y}_i = -1|d_i = +1) &= p_e \\ P(\hat{y}_i = +1|d_i = -1) &= p_e\end{aligned}$$

This results in the following metrices.
For $\hat{u} = 0 \longrightarrow d_i = +1$:

$$\begin{aligned}P(u=0) &= P(+1|+1)\cdot P(-1|+1)\cdot P(+1|+1)\cdot P_a(u=0) \\ &= (1-p_e)p_e(1-p_e)\frac{1}{4}\end{aligned}$$

For $\hat{u} = 1 \longrightarrow d_i = -1$:

$$\begin{aligned}P(u=1) &= P(+1|-1)\cdot P(-1|-1)\cdot P(+1|-1)\cdot P_a(u=1) \\ &= p_e(1-p_e)p_e\frac{3}{4}\end{aligned}$$

The decoder decides for $\hat{u} = 0$ if

$$\begin{aligned}P(u=0) &> P(u=1) \\ (1-p_e)p_e(1-p_e)\frac{1}{4} &> p_e(1-p_e)p_e\frac{3}{4} \\ 1-p_e &> 3p_e \\ 1 &> 4p_e \\ p_e &< \frac{1}{4}\end{aligned}$$

5.2 Introduction to Log-Likelihood Ratios

Consider log-likelihood ratios (L-values) of bits $u_k \in \{\pm 1\}$.

a) What is the probability $P(u_k = +1)$ if

(1) $L(u_k) = 0$
(2) $L(u_k) = \log_e(2)$
(3) $L(u_k) = -1$

Solution:

(1) $L(u_k) = 0$

$$
\begin{aligned}
L(u_k) &= \log \frac{P(u_k = +1)}{P(u_k = -1)} \\
e^{L(u_k)} &= \frac{P(u_k = +1)}{1 - P(u_k = +1)} \\
e^{L(u_k)} - e^{L(u_k)} \cdot P(u_k = +1) &= P(u_k = +1) \\
e^{L(u_k)} &= P(u_k = +1) + e^{L(u_k)} \cdot P(u_k = +1) \\
P(u_k = +1) &= \frac{e^{L(u_k)}}{1 + e^{L(u_k)}}
\end{aligned}
$$

Here, $L(u_k) = 0$:

$$P(u_k = +1) = \frac{e^0}{1 + e^0} = \frac{1}{2}$$

(2) $L(u_k) = \log_e(2)$

$$P(u_k = 1) = \frac{e^{\log_e(2)}}{1 + e^{\log_e(2)}} = \frac{2}{3}$$

(3) $L(u_k) = -1$

$$P(u_k = 1) = \frac{e^{-1}}{1 + e^{-1}} = \frac{1}{e + 1} \approx 0.27$$

b) A bit $u_k = +1$ is two times as likely as $u_k = -1$. Determine the log-likelihood ratio $L(u_k)$.

Solution:

$P(u_k = +1) = 2P(u_k = -1)$

$$\Rightarrow L(u_k) = \log_e \frac{P(u_k = +1)}{P(u_k = -1)} = \log_e \frac{2P(u_k = -1)}{P(u_k = -1)} = \log_e 2 \approx 0.69$$

c) Consider two bits with log-likelihood ratios $L(u_1) = -0.2$ and $L(u_2) = 20$. Determine the log-likelihood ratio $L(u_1 \oplus u_2)$ of the XOR combination $u_1 \oplus u_2$.

Solution:

Exact result:

$$
\begin{aligned}
L(u_1 \oplus u_2) = L(u_1) \boxplus L(u_2) &= \log_e \frac{e^{L(u_1)} e^{L(u_2)} + 1}{e^{L(u_1)} + e^{L(u_2)}} \\
&= \log_e \frac{e^{-0.2} e^{20} + 1}{e^{-0.2} + e^{20}} \approx -0.19999 \approx -0.2
\end{aligned}
$$

Approximation:

$$
\begin{aligned}
L(u_1 \oplus u_2) &= \operatorname{sign}(L(u_1)) \cdot \operatorname{sign}(L(u_2)) \cdot \min\{|L(u_1)|,\ |L(u_2)|\} \\
&= -1 \cdot 1 \cdot \min\{0.2,\ 20\} = -0.2
\end{aligned}
$$

In this case the approximation is very close to the exact value, as the magnitudes of $L(u_1)$ and $L(u_2)$ are very different.

d) Show that the probability $P(u_k = +1)$ can be expressed as

$$P(u_k = \pm 1) = \frac{e^{\frac{L(u_k)}{2}}}{1 + e^{L(u_k)}} e^{u_k \frac{L(u_k)}{2}}$$

Solution:

Proof:

To show the assumption consider first $u_k = +1$:

$$\begin{aligned} P(u_k = 1) &\overset{a)}{=} \frac{e^{L(u_k)}}{1 + e^{L(u_k)}} \\ &= \frac{e^{\frac{L(u_k)}{2}} e^{\frac{L(u_k)}{2}}}{1 + e^{L(u_k)}} \\ &\overset{u_k=+1}{=} \frac{e^{\frac{L(u_k)}{2}}}{1 + e^{L(u_k)}} e^{u_k \frac{L(u_k)}{2}} \end{aligned}$$

Proceed similarly for $u_k = -1$:

$$\begin{aligned} P(u_k = -1) &= 1 - P(u_k = 1) \\ &\overset{a)}{=} 1 - \frac{e^{L(u_k)}}{1 + e^{L(u_k)}} \\ &= \frac{1 + e^{L(u_k)} - e^{L(u_k)}}{1 + e^{L(u_k)}} \\ &= \frac{1}{1 + e^{L(u_k)}} \\ &= \frac{e^{\frac{L(u_k)}{2}} e^{-\frac{L(u_k)}{2}}}{1 + e^{L(u_k)}} \\ &\overset{u_k=-1}{=} \frac{e^{\frac{L(u_k)}{2}}}{1 + e^{L(u_k)}} e^{u_k \frac{L(u_k)}{2}} \end{aligned}$$

The expressions for $P(u_k = +1)$ and $P(u_k = -1)$ are the same. Note that only the sign of the exponent of the exponential function is changed depending on $u_k = \pm 1$

5.3 Soft-Output Decoder

a) A source generates statistical independent binary data $u_k \in \{\pm 1\}$, where $u_k = +1$ occurs with twice the probability of $u_k = -1$.

(1) Determine the log-likelihood ratio $L_a(u_k)$, that represents the statistics of the source.

Solution:

$$P(u_k = +1) = 2P(u_k = -1)$$

$$
\begin{aligned}
L_a(u_k) &= \log \frac{P(u_k = +1)}{P(u_k = -1)} \\
&= \log \frac{2P(u_k = -1)}{P(u_k = -1)} \\
&= \log 2 = 0.69
\end{aligned}
$$

Note that we define log-likelihood ratios using the natural logarithm $\log(\,\cdot\,) = \log_e(\,\cdot\,)$. This is advantageous for AWGN channels. In general also the $\log_2()$ could be used for L-values instead. In this case, we would obtain $L_a(u_k) = 1$.

(2) Determine the log-likelihood ratio $L(x)$, where the bit

$$x = u_1 \cdot u_2$$

is the product of two consecutive source bits u_1 and u_2.

Solution:

(2) Determine the log-likelihood ratio $L(x)$, where the bit

$$x = u_1 \cdot u_2$$

is the product of two consecutive source bits u_1 and u_2.

$$P(u_k = +1) = 2P(u_k = -1)$$

The bit $xu_1 \cdot u_2$ is the product of the source bits u_1 and u_2, which are statistically independent. Thus, we have

$$P(u_1, u_2) = P(u_1)P(u_2).$$

$$
\begin{aligned}
L(x) &= \log \frac{P(x = +1)}{P(x = -1)} \\
&= \log \frac{P(u_1 = +1)P(u_2 = +1) + P(u_1 = -1)P(u_2 = -1)}{P(u_1 = +1)P(u_2 = -1) + P(u_1 = -1)P(u_2 = +1)} \\
&= \log \frac{2P(u_1 = -1)2P(u_2 = -1) + P(u_1 = -1)P(u_2 = -1)}{2P(u_1 = -1)P(u_2 = -1) + P(u_1 = -1)2P(u_2 = -1)} \\
&= \log \frac{4+1}{2+2} = \log \frac{5}{4} = 0.22
\end{aligned}
$$

Again the $\log_2()$ could be used for L-values instead. In this case $L(x) = 0.32$.

$$L(x) = L(u_1 \oplus u_2) = L(u_1) \boxplus L(u_2)$$

The approximation

$$
\begin{aligned}
L(u_1 \oplus u_2) &= \operatorname{sign}(L(u_1)) \cdot \operatorname{sign}(L(u_2)) \cdot \min\{|L(u_1)|,\ |L(u_2)|\} \\
&= \operatorname{sign}(\log(2)) \cdot \operatorname{sign}(\log(2)) \cdot \min\{|\log(2)|,\ |\log(2)|\} \\
&= \log(2) = 0.69 \not\approx 0.22
\end{aligned}
$$

is not useful here, because $L(u_1) = L(u_2)$ and $|L(u_k)|$ is small.

b) A soft-output decoder determines a log-likelihood ratio of $L(\hat{u}) = -1$ for the information bit u.

(1) What is the hard decision $\hat{u}$ on the bit u.

Solution:

$$\hat{u} = \text{sign}\{L(\hat{u})\} = -1$$

The hard decision $\hat{u}$ for bit u is -1.

(2) Determine is the bit error probability P_b of the decoded bit $\hat{u}$? It can be estimated by the soft-output L-value of the decoder.

Solution: A soft output decoder delivers a soft output L-value $L(\hat{u})$. As the hard decision is $\hat{u} = \text{sign}\{L(\hat{u})\} = -1$ the decoder produces a bit error when the correct value of this bit was $u = +1$ and no error otherwise.

$$L(\hat{u}) = \log \frac{P(y = -1|u = +1)}{P(y = -1|u = -1)}$$
$$L(\hat{u}) = \log \frac{P_b}{1 - P_b} \stackrel{!}{=} -1$$

$$\Leftrightarrow e^{-1} = \frac{P_b}{1 - P_b}$$
$$\Leftrightarrow P_b = \frac{e^{-1}}{1 + e^{-1}} = \frac{1}{e + 1} = 0.2689$$

The bit error probability is 0.2689.

5.4 LLRs in AWGN Channel

A binary code of rate $R = \frac{1}{2}$ is used for a transmission over an AWGN channel. For the information word u the codeword $\mathbf{x} = \begin{bmatrix} x_1 & x_2 \end{bmatrix}^T$ is transmitted and $\mathbf{y} = \begin{bmatrix} y_1 & y_2 \end{bmatrix}^T$ is received.
Show that $L(\hat{u}) = L(u|y_1, y_2) = L(y_1|u) + L(y_2|u) + L_a(u)$ as the channel is memoryless.

Solution:

$$L(\hat{u}) = L(u|y_1, y_2) = \log \frac{p(u = +1|y_1, y_2)}{p(u = -1|y_1, y_2)}$$

$u_1 = +1$ is mapped to the codeword $\mathbf{x}^+$

$$u = +1 \rightarrow \mathbf{x}^+ = \begin{bmatrix} x_1^+ \\ x_2^+ \end{bmatrix}$$

$u_1 = -1$ is mapped to the codeword $\mathbf{x}^-$

$$u = -1 \rightarrow \mathbf{x}^- = \begin{bmatrix} x_1^- \\ x_2^- \end{bmatrix}$$

The a-posteriori distribution $p(u = \pm 1|y_1, y_2)$ is given by

$$P(u = \pm 1|y_1, y_2) = P(x_1^{\pm}, x_2^{\pm}|y_1, y_2)$$

using Bayes rule

$$= \frac{P(y_1, y_2|x_1^{\pm}, x_2^{\pm})P(x_1^{\pm}, x_2^{\pm})}{P(y_1, y_2)}$$

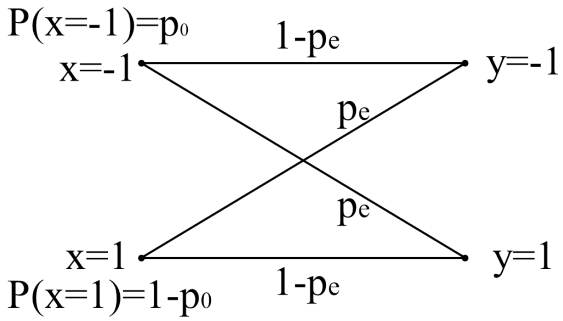
using the memoryless property of the AWGN channel $P(y_1, y_2|x_1^{\pm}, x_2^{\pm}) = P(y_1|x_1^{\pm})P(y_2|x_2^{\pm})$

and the mapping $u \to [x_1, x_2]^T$: $P(x_1^{\pm}, x_2^{\pm}) = P(u = \pm 1)$

$$\begin{aligned}
&= \frac{P(y_1|x_1^{\pm})P(y_2|x_2^{\pm})P(u = \pm 1)}{P(y_1, y_2)} \\
L(\hat{u}) &= \log \frac{P(y_1|x_1^{+})P(y_2|x_2^{+})P(u = +1)P(y_1, y_2)}{P(y_1|x_1^{-})P(y_2|x_2^{-})P(u = -1)P(y_1, y_2)} \\
&= \log \frac{P(y_1|x_1^{+})}{P(y_1|x_1^{-})} + \log \frac{P(y_2|x_2^{+})}{P(y_2|x_2^{-})} + \log \frac{P(u = +1)}{P(u = -1)} \\
&= \underbrace{L_c(x_1) \quad + \quad L_c(x_2)}_{\text{channel info}} \quad + \quad \underbrace{L_a(u)}_{\text{a-priori info}}
\end{aligned}$$

5.5 Binary Symmetric Channel, L-Values, ML, MAP

Consider a binary symmetric channel (BSC) with transmit symbols $x_k \in \{-1, +1\}$ and error probability $p_e = 0.1$.



a) Is the BSC a memoryless channel? Why?

Solution:

The BSC is a memoryless channel:

Consider transmission of a sequence of bits $\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. The received values are $\mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$. It holds, that

$$P(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} P(y_i|x_i)\,.$$

$\Rightarrow$ The channel is memoryless.

b) The uncoded binary data sequence $\mathbf{x} = \begin{bmatrix} x_1 & x_2 \end{bmatrix}^T = \begin{bmatrix} -1 & -1 \end{bmatrix}^T$ is transmitted through the BSC channel. Determine the probability that

(1) the sequence $\mathbf{y} = \begin{bmatrix} y_1 & y_2 \end{bmatrix}^T = \begin{bmatrix} +1 & -1 \end{bmatrix}^T$ is received.

Solution:

$$\begin{aligned} P\left(\mathbf{y} = \begin{bmatrix} +1 \\ -1 \end{bmatrix} \middle| \mathbf{x} = \begin{bmatrix} -1 \\ -1 \end{bmatrix}\right) &= p_e(1-p_e) \\ &= 0.1(1-0.1) \\ &= 0.09 \end{aligned}$$

(2) the sequence $\mathbf{y} = \begin{bmatrix} y_1 & y_2 \end{bmatrix}^T = \begin{bmatrix} -1 & +1 \end{bmatrix}^T$ is received.

Solution:

$$\begin{aligned} P\left(\mathbf{y} = \begin{bmatrix} -1 \\ +1 \end{bmatrix} \middle| \mathbf{x} = \begin{bmatrix} -1 \\ -1 \end{bmatrix}\right) &= (1-p_e)p_e \\ &= 0.9 \cdot 0.1 \\ &= 0.09 \end{aligned}$$

(3) both symbols are received error-free.

Solution:

$$\begin{aligned} P(\mathbf{y} = \mathbf{x}) &= (1-p_e)^2 \\ &= 0.9^2 \\ &= 0.81 \end{aligned}$$

c) The sequence $\mathbf{y} = \begin{bmatrix} y_1 & y_2 \end{bmatrix}^T = \begin{bmatrix} -1 & +1 \end{bmatrix}^T$ is received from the BSC. Assume that the transmit symbols $x_k = \pm 1$ are statistically independent and equally likely. Determine the probability that

(1) the sequence $\mathbf{x} = \begin{bmatrix} x_1 & x_2 \end{bmatrix}^T = \begin{bmatrix} -1 & -1 \end{bmatrix}^T$ was transmitted.

Solution:
Bayes rule:

$$P\left(\mathbf{x} = \begin{bmatrix} -1 \\ -1 \end{bmatrix} \middle| \mathbf{y} = \begin{bmatrix} -1 \\ +1 \end{bmatrix}\right) = P\left(\mathbf{y} = \begin{bmatrix} -1 \\ +1 \end{bmatrix} \middle| \mathbf{x} = \begin{bmatrix} -1 \\ -1 \end{bmatrix}\right) \frac{P\left(\mathbf{x} = \begin{bmatrix} -1 & -1 \end{bmatrix}^T\right)}{P\left(\mathbf{y} = \begin{bmatrix} -1 & +1 \end{bmatrix}^T\right)}$$

Since the transmit symbols are statistically independent, we have

$$P\left(\mathbf{x} = \begin{bmatrix} -1 \\ -1 \end{bmatrix}\right) = P(x_1 = -1)P(x_2 = -1) = \left(\frac{1}{2}\right)^2 = \frac{1}{4}.$$

As the channel is memoryless, we obtain

$$\begin{aligned} P\left(\mathbf{y} = \begin{bmatrix} -1 \\ +1 \end{bmatrix}\right) &= P(y_1 = -1) \cdot P(y_2 = +1) \\ &= (P(y_1 = -1|x_1 = -1)P(x_1 = -1) + P(y_1 = -1|x_1 = +1)P(x_1 = +1)) \\ &\quad \cdot (P(y_2 = +1|x = +1)P(x = +1) + P(y = +1|x = -1)P(x = -1)) \\ &= \left((1-p_e)\frac{1}{2} + p_e\frac{1}{2}\right) \cdot \left((1-p_e)\frac{1}{2} + p_e\frac{1}{2}\right) \\ &= \frac{1}{4}(1 - p_e + p_e)^2 = \frac{1}{4} \end{aligned}$$

$$P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right)=(1-p_e)p_e=0.09$$

$$\Rightarrow P\left(\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\middle|\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right)=P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right)\frac{P\left(\mathbf{x}=\begin{bmatrix}-1 & -1\end{bmatrix}^T\right)}{P\left(\mathbf{y}=\begin{bmatrix}-1 & +1\end{bmatrix}^T\right)}$$
$$=0.09\cdot\frac{\frac{1}{4}}{\frac{1}{4}}=0.09$$

(2) the sequence $\mathbf{x}=\begin{bmatrix}x_1 & x_2\end{bmatrix}^T=\begin{bmatrix}+1 & +1\end{bmatrix}^T$ was transmitted.

Solution:
Use again, that

$$P\left(\mathbf{x}=\begin{bmatrix}+1\\+1\end{bmatrix}\right)=P(x_1=+1)P(x_2=+1)=\left(\frac{1}{2}\right)^2=\frac{1}{4},$$

and

$$P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right)=\frac{1}{4}\text{ and }P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right)=(1-p_e)p_e=0.09.$$

Then, with Bayes rule we obtain

$$\Rightarrow P\left(\mathbf{x}=\begin{bmatrix}1\\1\end{bmatrix}\middle|\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right)=P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}1\\1\end{bmatrix}\right)\frac{P\left(\mathbf{x}=\begin{bmatrix}1 & 1\end{bmatrix}^T\right)]}{P\left(\mathbf{y}=\begin{bmatrix}-1 & +1\end{bmatrix}^T\right)}$$
$$=0.09\cdot\frac{\frac{1}{4}}{\frac{1}{4}}=0.09$$

d) Derive the probabilities from c) under the assumption that the probability of a transmit symbol $x_k=+1$ is three times the probability of a transmitted $x_k=-1$.

Solution:

$$\begin{aligned}&P(x=+1)=3P(x=-1)\\&P(x=+1)+P(x=-1)=1\Leftrightarrow P(x=+1)=1-P(x=-1)\\\Rightarrow&1-P(x=-1)=3P(x=-1)\\\Leftrightarrow&4P(x=-1)=1\\\Leftrightarrow&P(x=-1)=\frac{1}{4}\text{ and }P(x=+1)=\frac{3}{4}\end{aligned}$$

(1)

$$P\left(\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right)=P(x_1=-1)P(x_2=-1)=\left(\frac{1}{4}\right)^2=\frac{1}{16}$$

and

$$
\begin{aligned}
P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right) &= P(y_1=-1)P(y_2=+1)\\
&= (P(y_1=-1|x_1=-1)P(x_1=-1)+P(y_1=-1|x_1=+1)P(x_1=+1))\\
&\cdot (P(y_2=+1|x=+1)P(x=+1)+P(y=+1|x=-1)P(x=-1))\\
&= \left((1-p_e)\frac{1}{4}+p_e\frac{3}{4}\right)\cdot\left((1-p_e)\frac{3}{4}+p_e\frac{1}{4}\right)\\
&= \frac{1}{16}(1-p_e+3p_e)(3-3p_e+p_e)\\
&= \frac{1}{16}(1+2\cdot 0.1)(3-2\cdot 0.1) = 3.36\frac{1}{16} = 0.21
\end{aligned}
$$

$$
P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right) = (1-p_e)p_e = 0.09
$$

$$
\begin{aligned}
P\left(\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\middle|\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right) &= P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right)\frac{P\left(\mathbf{x}=\begin{bmatrix}-1 & -1\end{bmatrix}^T\right)}{P\left(\mathbf{y}=\begin{bmatrix}-1 & +1\end{bmatrix}^T\right)}\\
&= 0.09\cdot\frac{\frac{1}{16}}{3.36\frac{1}{16}}\\
&= 0.0268
\end{aligned}
$$

(2)

$$
P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right) = 3.36\cdot\frac{1}{16} = 0.21
$$

$$
P\left(\mathbf{x}=\begin{bmatrix}+1\\+1\end{bmatrix}\right) = P(x=+1)P(x=+1) = \frac{9}{16}
$$

$$
P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}-1\\-1\end{bmatrix}\right) = (1-p_e)p_e = 0.09
$$

$$
\begin{aligned}
P\left(\mathbf{x}=\begin{bmatrix}+1\\+1\end{bmatrix}\middle|\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\right) &= P\left(\mathbf{y}=\begin{bmatrix}-1\\+1\end{bmatrix}\middle|\mathbf{x}=\begin{bmatrix}+1\\+1\end{bmatrix}\right)\frac{P\left(\mathbf{x}=\begin{bmatrix}+1 & +1\end{bmatrix}^T\right)}{P\left(\mathbf{y}=\begin{bmatrix}-1 & +1\end{bmatrix}^T\right)}\\
&= 0.09\cdot\frac{\frac{9}{16}}{3.36\frac{1}{16}}\\
&= 0.2411
\end{aligned}
$$

e) Derive the general equation for an a-posteriori probability (APP) estimate and a maximum likelihood (ML) estimate using log-likelihood ratios.

Solution:

APP

$$\begin{aligned} L(\hat{x}_k) &= \log \frac{P(x_k=+1|y_k)}{P(x_k=-1|y_k)} \\ &= \log \frac{P(y_k|x_k=+1)P(x_k=+1)P(y_k)}{P(y_k|x_k=-1)P(y_k)P(x_k=-1)} \\ &= \underbrace{\log \frac{P(y_k|x_k=+1)}{P(y_k|x_k=-1)}}_{\substack{L_c(x_k) \\ \text{channel info}}} + \underbrace{\log \frac{P(x_k=+1)}{P(x_k=-1)}}_{\substack{L_a(x_k) \\ \text{a-priori info}}} \end{aligned}$$

ML

$$L(\hat{x}_k) = \underbrace{\log \frac{P(y_k|x_k=+1)}{P(y_k|x_k=-1)}}_{\substack{L_c(x_k) \\ \text{channel info}}}$$

f) Determine the APP and ML soft-output log-likelihood ratios as well as the respective hard decisions for the received sequence and the source statistics used in d).

Solution:

From d) we know that $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} -1 \\ +1 \end{bmatrix}$ and $P(x=-1) = \frac{1}{4}$ and $P(x=+1) = \frac{3}{4}$.

$$\left.\begin{matrix} P(x_k=+1) = \frac{3}{4} \\ P(x_k=-1) = \frac{1}{4} \end{matrix}\right\} \Rightarrow L_a(x_k) = \log \tfrac{P(x_k=+1)}{P(x_k=-1)} = \log \tfrac{\frac{3}{4}}{\frac{1}{4}} = \log 3$$

$$\begin{aligned} L_c(x_1) &= \log \frac{P(y_1=+1|x_1=+1)}{P(y_1=+1|x_1=-1)} \\ &= \log \frac{1-p_e}{p_e} = \log \frac{0.1}{0.9} \\ &= \log \frac{1}{9} \\ L_c(x_2) &= \log \frac{P(y_2=+1|x_2=+1)}{P(y_2=+1|x_2=-1)} \\ &= \log \frac{1-p_e}{p_e} = \log \frac{0.9}{0.1} \\ &= \log 9 \end{aligned}$$

APP soft output:

$$\begin{aligned} L(\hat{x}_1) &= L_c(x_1) + L_a(x_1) \\ &= \log \frac{1}{9} + \log 3 = -1.1 \\ L(\hat{x}_2) &= L_c(x_2) + L_a(x_2) \\ &= \log 9 + \log 3 = +3.3 \end{aligned}$$

APP hard decision:

$$\begin{aligned} \hat{x}_1 &= \operatorname{sign}\{L(\hat{x}_1)\} = -1 \\ \hat{x}_2 &= \operatorname{sign}\{L(\hat{x}_2)\} = +1 \end{aligned}$$

ML soft output:

$$L(\hat{x}_1) = L_c(x_1) = \log \frac{1}{9} = -2.2$$
$$L(\hat{x}_2) = L_c(x_2) = \log 9 = +2.2$$

ML hard decision:

$$\hat{x}_1 = \text{sign}\{L(\hat{x}_1)\} = -1$$
$$\hat{x}_2 = \text{sign}\{L(\hat{x}_2)\} = +1$$

Chapter 6

Linear Block Codes

6.1 Systematic $(3, 2, 2)_2$ Block Codes

Consider systematic $(3, 2, 2)_2$ block codes, where the information bits appear in original order as the first code bits.

a) Determine the code rate R.

Solution:

The parameters $(W, K, d_{\min})_q$ refer to

- the codeword length N,
- the information word length K,
- the minimum Hamming distance $d_{\min}$, and
- the code symbol alphabet size q.

The code rate is defined as the number of information symbols divided by the number of symbols of a codeword:

$$R = \frac{K}{N}$$

b) How many distinct $(3, 2, 2)_2$ block codes exist?

Solution:

A block code is defined by the set of codewords. $K = 2$ is the number of information bits. Thus there are 2^2 information words.

$$\mathbf{u} \in \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

$N = 3$ is the codeword length. As the codes are assumed to be systematic, one parity bit is after appended.

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ p_1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ p_2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ p_3 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ p_4 \end{bmatrix} \right\}$$

As $d_{min} = 2$ is the minimum distance, any two codewords must differ in at least two bits.

Comparing the first codeword with the second, we see that the information just differs in one bit and thus the parity bits must be different.

$$p_1 \neq p_2$$

In the same way, comparing the first with the third codebit leads to

$$p_1 \neq p_3 \,.$$

Comparing the first and the fourth codeword shows, that they differ in the two information bits and thus they satisfy the condition of $d_{min} = 2$ independent of the choice of p_4.

The same holds for p_2 and p_3, as the second and the third codeword differ in the two information bits.

Comparing now the second with the fourth codeword shows that they differ just in one information bit and therefore

$$p_2 \neq p_4 \,.$$

As in the third and fourth codeword there is just one different information bit it must be

$$p_3 \neq p_4 \,.$$

As every parity bit is either 1 or 0, there are just two possibilities to satisfy these conditions.

Choosing $p_1 = 0$ leads to $p_2 = p_3 = 1$ as they must be unequal of p_1 and $p_4 = 0$ as this must be unequal of p_3 and p_2. Alternatively for $p_1 = 1$ if follows that $p_2 = p_3 = 0$ and $p_4 = 1$.

Thus, we obtain two codes

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\} \quad \mathcal{C}_2 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

c) Are the codes from b) linear codes?

Solution:

A code is linear if the sum of any two codewords is again a codeword.

First consider the first code $\mathcal{C}_1 = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$:

As $\mathbf{x}_1 = 0 \in \mathcal{C}_1$ it holds that

$$\mathbf{x}_i + \mathbf{x}_i = \mathbf{0} \in \mathcal{C}_1$$

and

$$\mathbf{x_1} + \mathbf{x_i} = \mathbf{0} + \mathbf{x}_i = \mathbf{x}_i \in \mathcal{C}_1 \,.$$

But still we have to check whether the sum of any two of the other three codewords $\mathbf{x}_2,\ \mathbf{x}_3,\ \mathbf{x}_4$ is again a codeword.

$$\begin{aligned} \mathbf{x_2} + \mathbf{x_3} &= \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T + \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}^T && = \mathbf{x_4} \in \mathcal{C}_1 \\ \mathbf{x_2} + \mathbf{x_4} &= \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T + \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^T && = \mathbf{x_3} \in \mathcal{C}_1 \\ \mathbf{x_3} + \mathbf{x_4} &= \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^T + \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}^T = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}^T && = \mathbf{x_2} \in \mathcal{C}_1 \end{aligned}$$

$\Rightarrow \mathcal{C}_1$ is linear.

Now consider the second code $\mathcal{C}_2 = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$:

As $0 \notin \mathcal{C}_2$, it follows directly that $\mathbf{x}_i + \mathbf{x}_i = \mathbf{0} \notin \mathcal{C}_2$, and therefore, the code $\mathcal{C}_2$ is not linear.

Alternatively, this can be shown by taking any sum of codewords, which is not in $\mathcal{C}_2$, e.g.

$$\begin{bmatrix}0 & 1 & 0\end{bmatrix}^T + \begin{bmatrix}1 & 0 & 0\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 0\end{bmatrix}^T \notin \mathcal{C}_2\,.$$

6.2 Binary Code of Length $N = 5$

A binary code of length $N = 5$ is used for the transmission of data symbols. The encoder maps the data symbols to vectors of length 5 bits, where exactly 3 bits have value '1'.

a) How many codewords exist?

Solution:

The number of codewords is the same as the number of possibilities to choose the positions of the 3 ones out of the 5 possible positions.

$$\binom{5}{3} = \frac{5!}{(5-3)! \cdot 3!} = 10$$

b) State all codewords of this code. What is the minimum Hamming distance of the code?

Solution:

$$\mathcal{C} = \left\{ \begin{bmatrix}0\\0\\1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\\1\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix} \right\}$$

To determine d_{min}, take for example the last two codewords.

$$d_H\left(\begin{bmatrix}1 & 1 & 0 & 1 & 0\end{bmatrix}^T, \begin{bmatrix}1 & 1 & 1 & 0 & 0\end{bmatrix}^T\right) = 2$$

Thus $d_{min} \leq 2$ and as there are no two codewords with Hamming distance of 1, the minimum Hamming distance is

$$d_{min} = 2\,.$$

Alternative solution:
The number of ones and zeros in every codeword is fixed. Suppose two codewords, which have a zero in the same position. Then the second zero must be placed in different position in order to obtain a different codeword. Thus, the first codeword has a '0' where the second codeword has a '1' (first difference) and the second codeword also has a '0' where the first codeword has a '1' (second difference). Thus every two codewords have a Hamming distance of at least 2 and therefore $d_{min} = 2$.

c) Is this code a linear code?

Solution:

The code does not contain the all-zero codeword $\mathbf{0}$. Thus $\mathbf{x}_i + \mathbf{x}_i = \mathbf{0}$ is not a codeword.

$$\Rightarrow \text{ The code is not linear.}$$

Alternative solution:
Consider for example $\begin{bmatrix}1 & 1 & 0 & 1 & 0\end{bmatrix}^T + \begin{bmatrix}1 & 1 & 1 & 0 & 0\end{bmatrix}^T = \begin{bmatrix}0 & 0 & 1 & 1 & 0\end{bmatrix}^T$ which is not an element of the code. Obviously, is the sum of two codewords is not always a codeword, and therefore, the code is not linear.

6.3 Single-Parity-Check-Code and Dual Code

Consider a $(N,\ N-1)_2$ Single-Parity-Check-Code (SPC-Code).

a) Determine the code rate R.

Solution:

$$R = \frac{K}{N} = \frac{N-1}{N} = 1 - \frac{1}{N}$$

b) Determine the minimum Hamming Distance d_{min} depending on N.

Solution:

$$d_{min} = 2 \text{ (SPC Code)}$$

c) How many bit errors can at least be detected by a $(N,\ N-1)_2$ SPC-Code?

Solution:

$$d_{min} - 1 = 2 - 1 \text{ errors can be detected.}$$

d) How many bit errors can at least be corrected by a $(N,\ N-1)_2$ SPC-Code?

Solution:

$$\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{2-1}{2} \right\rfloor = 0 \text{ errors can be corrected.}$$

For the following parts e) - l), consider the special case $N = 4$.

e) State all codewords of the SPC-codes.

Solution:

	information			parity
	u_1	u_2	u_3	p
x_1	0	0	0	0
x_2	0	0	1	1
x_3	0	1	0	1
x_4	0	1	1	0
x_5	1	0	0	1
x_6	1	0	1	0
x_7	1	1	0	0
x_8	1	1	1	1

f) Determine a generator matrix $\mathbf{G}_{SPC}$ of the SPC-code.

Solution:

$\mathbf{x} = \mathbf{G}_{SPC} \cdot \mathbf{u}$

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

g) Determine a parity check matrix $\mathbf{H}_{SPC}$ of the SPC-code.

Solution:

$\mathbf{H}_{SPC}$ is a $N \times N - K = 4 \times 4 - 3 = 4 \times 1$ matrix.

$$\mathbf{H}_{SPC} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

h) Determine the product $\mathbf{H}_{SPC}^T \cdot \mathbf{G}_{SPC}$ of the parity check matrix $\mathbf{H}_{SPC}$ and the generator matrix $\mathbf{G}_{SPC}$.

Solution:

$$\begin{array}{ccccc} \mathbf{H}_{SPC}^T & \cdot & \mathbf{G}_{SPC} & = & \mathbf{0} \\ N-K \times N & \cdot & N \times K & = & N-K \times K \\ 1 \times 4 & \cdot & 4 \times 3 & = & 1 \times 3 \end{array}$$

i) Derive the Maximum-Likelihood (ML) decoding rule for the SPC-Code for transmission over an AWGN channel. Simplify the expression as much as possible!

Solution:

$$
\begin{aligned}
\hat{\mathbf{u}} &= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmax}} P(\mathbf{y}|\mathbf{x}) \\
&= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmax}} \prod_{i=1}^{N} p(y_i|x_i) \\
&\text{(since the AWGN channel is memoryless)} \\
&= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmax}} \log\left(\prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma_N^2}} \exp\left(-\frac{(y_i-x_i)^2}{2\sigma_N^2}\right)\right) \\
&\text{(logarithm of object function does not change the result of the maximization)} \\
&= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmax}} \left(\sum_{i=1}^{N}\left(-\frac{(y_i-x_i)^2}{2\sigma_N^2}\right) - \log(\sqrt{2\pi\sigma_N^2})\right) \\
&\text{(the second term of the sum is constant for all } x_i\text{,} \\
&\text{and thus, it can be dropped for maximization)} \\
&= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmin}} \sum_{i=1}^{N}(y_i-x_i)^2 \\
&= \underset{\mathbf{u}\to\mathbf{x}}{\operatorname{argmin}} \sum_{i=1}^{N}(y_i^2 - 2y_ix_i + x_i^2)
\end{aligned}
$$

With $\hat{x}_i \in \{\pm 1\}$ and $y_i \in \{\pm 1\}$

$$
= \arg\max_{\mathbf{u}\to\mathbf{x}} \sum_{i=1}^{N} y_i x_i
$$

The dual code $\mathcal{C}^{\perp}$ corresponding to the code $\mathcal{C}$ is defined as the code which is generated by switching the roles of generator matrix and parity check matrix, i.e.

$$
\mathbf{G}_{SPC}^{\perp} = \mathbf{H}_{SPC}\,.
$$

j) Determine the code rate $R^{\perp}$ of the dual code of the $(N,\ N-1)_2 = (4,\ 3)_2$ SPC-Code.

Solution:

$$
\mathbf{G}_{SPC}^{\perp} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}
$$

$$
\Rightarrow R^{\perp} = \frac{1}{N} = \frac{1}{4}
$$

k) Which well known block code is this dual code?

Solution:

Repetition code

l) Determine the minimum Hamming distance $d_{min}^{\perp}$ of the dual code $\mathcal{C}^{\perp}$.

Solution:

$$d_{min}^{\perp} = N = 4$$

m) Now, consider a general $(N,\ K)_2$ code $\mathcal{C}$. What is the code rate $R_{\mathcal{C}^\perp}$ of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ depending on N and K.

Solution:

$\mathbf{G}_{SPC}^{\perp}$ is a $N \times N-K$-matrix.

$$\Rightarrow R_{\mathcal{C}^\perp} = \frac{N-K}{N} = 1 - \frac{K}{N} = 1 - R_C$$

6.4 Existence of an $(N,\ K,\ d_{min})_2$

Consider a linear $(N,\ K,\ d_{min})_2$ block code.

a) How many bit errors can a code with minimum Hamming distance $d_{min} = 5$ always correct?

Solution:

$$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{5-1}{2} \right\rfloor = \frac{4}{2} = 2$$

2 errors can be corrected.

b) How many bit errors can a code with minimum Hamming distance $d_{min} = 5$ always detect?

Solution:

$$t' = d_{min} - 1 = 5 - 1 = 4$$

4 errors can be detected.

c) Can a linear $(10,\ 8,\ 5)_2$ block code exist? Explain your answer!

Solution:

All existing codes have to satisfy the Singleton Bound and the Hamming Bound:
Singleton Bound:

$$d_{min} \leq N - K + 1$$

$$\begin{aligned} d_{min} &\leq N - K + 1 \\ 5 &\overset{?}{\leq} 10 - 8 + 1 \\ 5 &\overset{?}{\leq} 3 \quad \lightning \end{aligned}$$

The Singleton bound is violated. Therefore, such a code can not exist.

Alternative solution - Hamming bound:

$$
\begin{aligned}
q^{N-K} &\geq \sum_{r=0}^{t} \binom{N}{r} (q-1)^r \\
N-K &\geq \log_q \left(\sum_{r=0}^{t} \binom{N}{r} (q-1)^r \right) \\
10-8 &\overset{?}{\geq} \log_2 \left(\sum_{r=0}^{2} \binom{10}{r} (2-1)^r \right) \\
2 &\overset{?}{\geq} \log_2 \left(\binom{10}{0} + \binom{10}{1} + \binom{10}{2} \right) \\
2 &\overset{?}{\geq} \log_2 \left(1 + 10 + \frac{10!}{8! \cdot 2!} \right) \\
2 &\overset{?}{\geq} \log_2 56 = 5.8 \quad \lightning
\end{aligned}
$$

The hamming bound is violated. Therefore, such a code cannot exist.

6.5 Hamming Code

In this task a $(7,\ 4,\ 3)$ Hamming code with the following generator matrix is considered:

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

a) Is this Hamming code a systematic code?

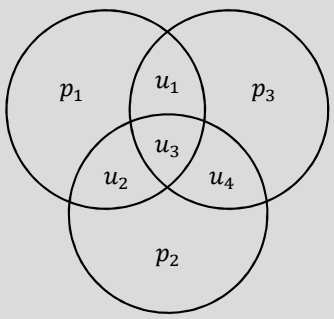
Solution:

The Hamming code is systematic as the code bits $x_1, \vdots, x_4$ are equal to the information bits $u_1, \vdots, u_4$.
This can also be seen from the identity matrix in the upper part of $\mathbf{G}$:

$$
\mathbf{x} = \mathbf{G}\mathbf{u} = \begin{bmatrix} \mathbf{I}_{4\times 4} \\ \mathbf{P} \end{bmatrix} \mathbf{u} = \begin{bmatrix} \mathbf{u} \\ \mathbf{p} \end{bmatrix}
$$

b) Determine a parity check matrix $\mathbf{H}$ for this Hamming code.

Solution:



Each circle represents one check equation.

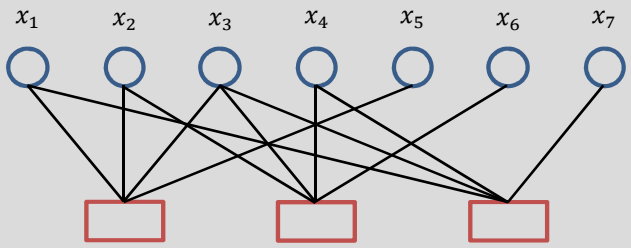
$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Alternatively:

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_{4\times 4} \\ \mathbf{P} \end{bmatrix} \quad \Rightarrow \quad \mathbf{H}^T = \begin{bmatrix} -\mathbf{P} & \mathbf{I}_{3\times 3} \end{bmatrix}$$

c) Sketch the Tanner graph characterizing this Hamming code.

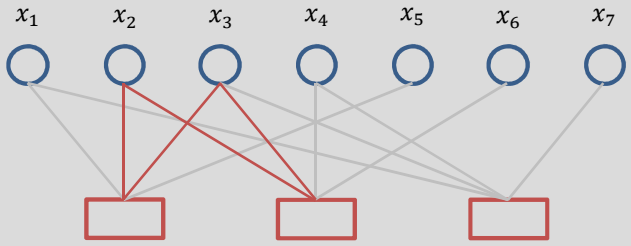
Solution:



d) What is the girth of a Tanner graph? Determine the girth of the graph in task c)

Solution:

The girth descibes the length of the shortest cycle in the Tanner graph. In this case the girth is 4:



e) Can message-passing decoding be a maximum likelihood decoding in the case of this Hamming code?

Solution:

Message passing decoding is the maximum likelihood decoding when the Tanner graph has no cycle at all.

As the girth for this code is 4 message passing decoding is not maximum likelihood decoding for the Hamming code.

f) How many bit errors t can at least be corrected by this code?

Solution:

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{3 - 1}{2} \right\rfloor = 1$$

g) Determine the probability that more than t errors occur in a BSC with error probability p_e, when taking the error correction capabilities of the code into account.

Solution:

The output of a binary symmetrical channel can be divided into the sum of two parts: A sequence $\boldsymbol{x}$ where no errors occur and into an error sequence $\boldsymbol{e}$.

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

$\boldsymbol{x}$ can be any element of the set of codewords $\mathcal{C}$, where each codeword has length N. Thus, at maximum N errors in one frame can occur.

The number of errors in $\boldsymbol{e}$ is given by the hamming wheight $w_H(\boldsymbol{e})$, which counts the number of ones.

Thus, the probability p_{error} that more than t errors occur after decoding, is written as

$$p_{\text{error}} = p(w_H(\mathbf{e}) > t)$$

Further, $p(w_H(\mathbf{e}) > t)$ can be formulated as

$$p(w_H(\mathbf{e}) > t) = \sum_{i=t+1}^{N} p(w_H(\mathbf{e}) = i)$$

Considering $\boldsymbol{e}$ as a sequence resulting from a Bernoulli process, we can create a tree diagramm. The probability $p(w_H(\mathbf{e}) = i)$ is equal to the sum of all branch probabilities with i elements equal to one. Due to the independence between all elements of $\boldsymbol{e}$, the branch probability is $p_e^i(1-p_e)^{N-i}$.

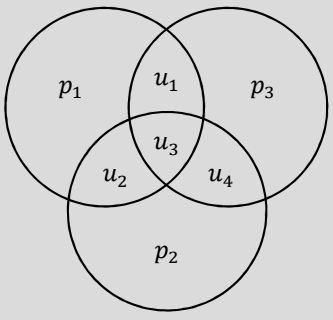
The number of branches having i ones is given by the Bernoulli coeffcient $\binom{N}{i} = \frac{N!}{(N-i)!i!}$.

Thus, applying all derived relationships yields

$$\begin{aligned} p_{\text{error}} = p(w_H(\mathbf{e}) > t) &= \sum_{i=t+1}^{N} \binom{N}{i} p_e^i (1-p_e)^{N-i} \\ &= 1 - \sum_{i=0}^{t} \binom{N}{i} p_e^i (1-p_e)^{N-i} \end{aligned}$$

h) How many bit erasures can at least be corrected in a binary erasure channel (BEC)?

Solution:



Each check equation can correct single erasures as the correct value can be reproduced from the others. Whenever there are two erasures in one check equation one of them has to be corrected by another equation. As long as there are only two erasures this is feasible. However, it is possible to position three erasures in such a way, that all check equation include at least two of them. So at least 2 erasures are correctable.

6.6 Reed-Muller Codes of First Order

A $RM(1,\ m)$ Reed-Muller Code of first order is determined by the following generator matrix:

$$\mathbf{G}_{1,m} = \begin{bmatrix} \mathbf{G}_{1,m-1} & \mathbf{0} \\ \mathbf{G}_{1,m-1} & \mathbf{1}_{2^{m-1},1} \end{bmatrix},$$

where $\mathbf{1}_{2^{m-1},1} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$ is a $(2^{m-1} \times 1)$ vector containing only ones.

For initialization, $\mathbf{G}_{1,1}$ is chosen to be the (2×2) identity matrix $\mathbf{I}_2$.

a) Determine the generator matrix $\mathbf{G}_{1,2}$ of a $RM(1,\ 2)$ code (i.e. $m = 2$).

Solution:

With $\mathbf{G}_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\mathbf{G}_{1,2} = \begin{bmatrix} \mathbf{G}_{1,1} & \mathbf{0} \\ \mathbf{G}_{1,1} & \mathbf{1}_{2^1,1} \end{bmatrix}$, we obtain

$$\mathbf{G}_{1,2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

b) Does the generator matrix from a) represent a systematic encoder? Explain your answer!

Solution:

$\mathbf{G}_{1,2}$ does not represent a systematic encoder, because the (3×3) identity matrix is not explicitly contained in $\mathbf{G}_{1,2}$.

c) Determine the code rate R of the $RM(1,\ 2)$ code?

Solution:

$$R = \frac{K}{N} = \frac{3}{4}$$

d) State all codewords of the $RM(1,\ 2)$ code.

Solution:

information word $\mathbf{u}$			codeword $\mathbf{c}$			
0	0	0	0	0	0	0
0	0	1	0	0	1	1
0	1	0	0	1	0	1
0	1	1	0	1	1	0
1	0	0	1	0	1	0
1	0	1	1	0	0	1
1	1	0	1	1	1	1
1	1	1	1	1	0	0

e) Is the RM(1, 2) code a linear code? Explain your answer!

Solution:

A code is linear if the sum of any two codewords is again a codeword.

As $\mathbf{x}_1 = \mathbf{G}_{1,2}\mathbf{u}_1$ and $\mathbf{x}_2 = \mathbf{G}_{1,2}\mathbf{u}_2$, it holds that

$$\mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{G}_{1,2}\mathbf{u}_1 \oplus \mathbf{G}_{1,2}\mathbf{u}_2 = \mathbf{G}_{1,2}(\mathbf{u}_1 \oplus \mathbf{u}_2)$$

$\Rightarrow$ The modulo-2-sum of any two codewords is again a codeword.
$\Rightarrow$ The code is linear.

f) Determine the minimum Hamming distance d_{min} of the $RM(1,\ 2)$ code?

Solution:

$$d_{min} = \min_{\mathbf{x}_i, \mathbf{x}_j \in RM(1,\ 2)} \{d_H(\mathbf{x}_i, \mathbf{x}_j)\}$$

For a linear block code, the minimum Hamming distance $d_{\min}$ is equal to the minimum Hamming weight $w_{\min}$, ie.e $d_{\min} = w_{\min} = 2$.

g) How many errors can a $RM(1,\ 2)$ code always detect? Explain your answer!

Solution:

$$d_{min} - 1 = 2 - 1 = 1$$

errors can be detected.

h) How many errors can a $RM(1,\ 2)$ code always correct? Explain your answer!

Solution:

$$\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{2 - 1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$$

errors can corrected.

i) State the Hamming-weight distribution of the $RM(1,\ 2)$ code.

Solution:

Use the table of d) and determine the weight of each codeword:

information word $\mathbf{u}$	codeword $\mathbf{c}$	Hamming weight w_H
0 0 0	0 0 0 0	0
0 0 1	0 0 1 1	2
0 1 0	0 1 0 1	2
0 1 1	0 1 1 0	2
1 0 0	1 0 1 0	2
1 0 1	1 0 0 1	2
1 1 0	1 1 1 1	4
1 1 1	1 1 0 0	2

Therefore, we have the weight distribution:

Hamming weight $w_H(w)$	quantity A_w
0	1
1	0
2	6
3	0
4	1

$\Rightarrow$ weight enumerator polynomial: $A(z) = \sum_{w=0}^{N} A_w z^w = 1 \cdot z^0 + 6 \cdot z^2 + 1 \cdot z^4 = 1 + 6z^2 + z^4$

j) Show that the $RM(1,\ 2)$ code is a Single-Parity-Check code.

Solution:

All codewords have even Hamming weight.

$\Rightarrow$ The $\oplus$-sum over all codewords is 0. Additionally, $R = \frac{K}{K+1}$.

$\Rightarrow$ The $RM(1,\ 2)$ code is a Single-Parity-Check code.

k) Derive the generator matrix of a systematic $(4,\ 3,\ 2)_2$- Single-Parity-Check code by elementary column operations on the generator matrix $\mathbf{G}_{1,2}$ of a $RM(1,\ 2)$ code.

Solution:

$$\mathbf{G}_{1,2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Targeted:

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

Substitute the first column in $\mathbf{G}_{1,2}$ by the $\oplus$-sum of the 1. and 3. column:

$$\mathbf{G'}_{1,2} = \begin{bmatrix} 1 \oplus 0 & 0 & 0 \\ 0 \oplus 0 & 1 & 0 \\ 1 \oplus 1 & 0 & 1 \\ 0 \oplus 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \mathbf{G}_{SPC}$$

l) Determine a parity check matrix $\mathbf{H}$ of a $RM(1,\ 2)$ code.

Solution:

$$\mathbf{H}^T \cdot \mathbf{G}_{1,2} = \mathbf{0}$$

$\mathbf{H}^T$ is a $N - K \times N = 1 \times 4$ matrix of rank $rank(\mathbf{H}^T) = N - K = 4 - 3 = 1$ and each $d_{min} - 1 = 2 - 1 = 1$ columns are linear independent.

Claim: $\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$ satisfies all conditions.
Proof: $\mathbf{H}^T$ is a 1×4 matrix of rank$(H^T) = 1$. Each column is $\neq \mathbf{0}$.

$$\mathbf{H}^T\mathbf{G}_{1,2} = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

$\Rightarrow \mathbf{H}^T = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$ is a parity check matrix of $\mathbf{G}_{1,2}$.
Since $\mathbf{G}_{SPC}$ is a different encoder for the same code,

$$\mathbf{H}^T\mathbf{G}_{SPC} = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$$

does also hold.

m) The dual code $\mathcal{C}^\perp$ of a code $\mathcal{C}$ is obtained if the roles of generator matrix and parity check matrix are exchanged. Which code is the dual code of a $RM(1,\ 2)$ code?

Solution:

$$\mathbf{G}_{1,2}^\perp = \mathbf{H} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

$\Rightarrow$ The dual code $\mathcal{C}^\perp$ is a repetition code with rate $R = \frac{1}{4}$.

6.7 Properties of Linear Block Codes

The code $\mathcal{C}$ consists of the following codewords:

$$\mathbf{x}_1 = \begin{bmatrix}0\\0\\0\\0\\0\end{bmatrix},\ \mathbf{x}_2 = \begin{bmatrix}1\\1\\0\\1\\0\end{bmatrix},\ \mathbf{x}_3 = \begin{bmatrix}0\\0\\1\\1\\1\end{bmatrix},\ \mathbf{x}_4 = \begin{bmatrix}1\\1\\1\\0\\1\end{bmatrix}.$$

a) Is the code $\mathcal{C}$ linear?

Solution:

A code is linear if the sum of any two codewords is again a codeword.

$\mathbf{x}_1 + \mathbf{x}_i = \mathbf{x}_i \in \mathcal{C}$
$\mathbf{x}_i + \mathbf{x}_i = \mathbf{x}_1 \in \mathcal{C}$
$\mathbf{x}_2 + \mathbf{x}_3 = \begin{bmatrix}1 & 1 & 0 & 1 & 0\end{bmatrix}^T + \begin{bmatrix}0 & 0 & 1 & 1 & 1\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 1 & 0 & 1\end{bmatrix}^T = \mathbf{x}_4 \in \mathcal{C}$
$\mathbf{x}_2 + \mathbf{x}_4 = \begin{bmatrix}1 & 1 & 0 & 1 & 0\end{bmatrix}^T + \begin{bmatrix}1 & 1 & 1 & 0 & 1\end{bmatrix}^T = \begin{bmatrix}0 & 0 & 1 & 1 & 1\end{bmatrix}^T = \mathbf{x}_3 \in \mathcal{C}$
$\mathbf{x}_3 + \mathbf{x}_4 = \begin{bmatrix}0 & 0 & 1 & 1 & 1\end{bmatrix}^T + \begin{bmatrix}1 & 1 & 1 & 0 & 1\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 0 & 1 & 0\end{bmatrix}^T = \mathbf{x}_2 \in \mathcal{C}$

The sum of any two codewords is also a codeword. $\Rightarrow$ the code is linear.

b) Determine the minimum Hamming distance d_{min}.

Solution:

$$
\begin{aligned}
d_H(\mathbf{x}_1, \mathbf{x}_2) &= 3 \\
d_H(\mathbf{x}_1, \mathbf{x}_3) &= 3 \\
d_H(\mathbf{x}_1, \mathbf{x}_4) &= 4 \\
d_H(\mathbf{x}_2, \mathbf{x}_3) &= 4 \\
d_H(\mathbf{x}_2, \mathbf{x}_4) &= 3 \\
d_H(\mathbf{x}_4, \mathbf{x}_3) &= 3
\end{aligned}
$$

The minimum Hamming distance is

$$d_{min} = \min_{i \neq j} d_H(\mathbf{x}_i, \mathbf{x}_j) = 3.$$

c) How many bit errors can at least be detected by the code $\mathcal{C}$?

Solution:

The code $\mathcal{C}$ can recognize at least

$$d_{min} - 1 = 3 - 1 = 2$$

errors.

d) How many bit errors can at least be corrected by the code $\mathcal{C}$?

Solution:

The code $\mathcal{C}$ can correct at least

$$\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{3 - 1}{2} \right\rfloor = 1 \tag{6.1}$$

errors.

e) Determine the code rate R?

Solution:

Each codeword has 5 bits $\Rightarrow N = 5$. There are 4 codewords, and therefore, also 4 information words. Consequently, each information word contains $K = \log_2 4\text{bit}$. The code rate is

$$R = \frac{K}{N} = \frac{2}{5}.$$

f) Which of the following matrices are parity check matrices for the code $\mathcal{C}$? Give reason.

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad \mathbf{H}_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{H}_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad \mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Solution:

- A parity check matrix has the dimensions $N \times N - K = 5 \times 3$. $\Rightarrow \mathbf{H}_4$ is no parity check matrix.
- A parity check matrix satisfies $\mathbf{H}\mathbf{x}_i$ for all valid codewords $\mathbf{x}_i, \quad i = 1, 2, 3, 4$. This

condition is satisfied for $\mathbf{H}_1$ and $\mathbf{H}_3$.For $\mathbf{H}_2$ e.g. $\mathbf{H}_2^T \cdot \mathbf{x}_4 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \neq \mathbf{0}$. $\Rightarrow \mathbf{H}_2$ is no parity check matrix.

- The rank of $\mathbf{H}$ must be $N - K = 3$. The rank of $\mathbf{H}_1$ is 3. The rank of $\mathbf{H}_3$ is 2. $\Rightarrow$ $\mathbf{H}_3$ is no parity check matrix.
- Any $d_{min} - 1 = 2$ rows of $\mathbf{H}_1$ are linear independent. $\Rightarrow \mathbf{H}_1$ is a parity check matrix.

g) Determine the product of $\mathbf{H}^T \cdot \mathbf{G}$ for the parity check matrix $\mathbf{H}$ found in f) and the generator matrix $\mathbf{G}$ of the code $\mathcal{C}$.

Solution:

$\mathbf{H}^T \cdot \mathbf{G} = 0$ for any pair of parity check and generator matrix.

h) Determine a mapping of the information vectors $\mathbf{u}_i$ to the codewords $\mathbf{x}_i$ of code $\mathcal{C}$ for a non systematic encoder.

Solution:

e.g.

$$\begin{aligned} \mathbf{u}_1 &= \begin{bmatrix} 0 & 0 \end{bmatrix}^T \mapsto \mathbf{x}_4 \\ \mathbf{u}_2 &= \begin{bmatrix} 0 & 1 \end{bmatrix}^T \mapsto \mathbf{x}_1 \\ \mathbf{u}_3 &= \begin{bmatrix} 1 & 0 \end{bmatrix}^T \mapsto \mathbf{x}_2 \\ \mathbf{u}_4 &= \begin{bmatrix} 1 & 1 \end{bmatrix}^T \mapsto \mathbf{x}_3 \end{aligned}$$

With a systematic encoder, information word appears explicitly in the codeword. E.g., the information word is the first part of a codeword and additional parity bits are appended. As for example, $\mathbf{x}_4$ contains only one 0, the information word $\mathbf{u}_1 = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$ is not contained directly in $\mathbf{x}_4$.

6.8 Shortening of Linear Block Codes

Sometimes, it is not possible to find a code of suitable codeword length or information word length for a given application. Therefore, it is desirable to construct a suitable code by shortening or extension of a known code. We will investigate the strategy of code shortening for the example of a $(7, 4, 3)_2$ Hamming code. The parity check matrix $\mathbf{H}$ of the Hamming code is given by

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

a) Determine the codeword length N of the Hamming code.

Solution:

According to the tuple $(7, 4, 3)_2$ denoting the properties of the given code, the codeword length is $N = 7$.

b) Determine the code rate R of the Hamming code.

Solution:

According to the tuple $(7, 4, 3)_2$ denoting the properties of the given code, the number of information bits K is $K = 4$. Thus, the rate can be computed

$$R = \frac{K}{N} = \frac{4}{7}$$

c) Determine the minimum Hamming distance $d_{\min}$ of the Hamming code.

Solution:

According to the tuple $(7, 4, 3)_2$ denoting the properties of the given code, the minimum Hamming distance $d_{\min}$ is $d_{\min} = 3$.

d) Determine the number of parity checks which are defined in the parity check matrix $\mathbf{H}$.

Solution:

The number of parity checks equals the number of columns of $\mathbf{H}$. Thus, the number of parity checks is 3.

e) Derive a systematic generator matrix $\mathbf{G}$ from the parity check matrix $\mathbf{H}$. The information bits shall appear in original order as the first bits of the codeword. Make sure that each step in your derivation is clearly given.

Solution:

At first, to obtain a systematic generator matrix, the parity matrix has to be transformed in the form

$$\mathbf{H}_{\text{sys}} = \begin{bmatrix} \mathbf{P}^T \\ \mathbf{I} \end{bmatrix}. \tag{6.2}$$

Summation of the first and second column of $\mathbf{H}$ yields a new first coloumn

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

In a second step, the second and third column of $\mathbf{H}_1$ are summed up to create a new second column

$$\mathbf{H}_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Finally, addition of the first and second column of $\mathbf{H}_2$ to obtain a new second column

and addition of the first and third column of $\mathbf{H}_2$ to obtain a new third column yields

$$\mathbf{H}_{\text{sys}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The parity check matrix $\mathbf{H}$ and the generator matrix $\mathbf{G}$ are orthogonal, i.e.

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

Since, after modification, the parity check matrix is in the form

$$\mathbf{H}_{\text{sys}} = \begin{bmatrix} \mathbf{P}^T \\ \mathbf{I} \end{bmatrix} \tag{6.3}$$

an systematic generator matrix can be found as

$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} \mathbf{I} \\ \mathbf{P} \end{bmatrix}. \tag{6.4}$$

It can be easily shown that $\mathbf{H}_{\text{sys}}^T\mathbf{G}_{\text{sys}} = \mathbf{0}$. Hence, the desired systematic generator matrix is

$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

The set of codewords of the $(7, 4, 3)_2$ Hamming code is summarized in the following table:

0000000	*0100101*	*1000011*	*1100110*
0001111	*0101010*	*1001100*	*1101001*
0010110	*0110011*	*1010101*	*1110000*
0011001	*0111100*	*1011010*	*1111111*

In the following problems f)-j), we consider code shortening. The codeword length and the information word length of the original code are denoted by N and K, respectively. For shortening of the code, the shortened code consists only of a subset of the codewords in the table above. For the shortened code, we choose only those codewords, which have M leading zeros. The M leading zeros are then deleted in order to obtain codewords of length $N - M$.

f) Determine the information word length of the shortened code depending on K and M.

Solution:

In general, a code with a binary alphabet and K information bits has 2^K valid codewords. However, in this case, due to the shortening 2^M codewords are dropped and thus the number of codewords decreases to 2^{K-M}. Consequently, the new information word

length is $K - M$.

g) Determine the code rate R_S of the shortened code depending on N, K and M.

Solution:

As derived in the previous subtask, the new information word length is $K-M$. Similarly, the codeword length is also reduced due to shortening, i.e. $N_S = N - M$. The resulting rate is

$$R_s = \frac{K - M}{N - M} \tag{6.5}$$

h) What is the impact of code shortening on the minimum Hamming distance. Give clear reasons for your answer.

Solution:

For linear codes, the minimum Hamming distance $d_{\min}$ is equal to the minimum Hamming weight $w_{\min}$. Since only code bits with value 0 are dropped, the minimum Hamming weight and consequently the minimum Hamming distance cannot become smaller. However, codewords of the original code with minimum Hamming weight could be excluded. Therefore, the shortened code will have at least the same minimum Hamming distance as the original code, i.e.

$$d_{\min,\mathrm{s}} \geq d_{\min}.$$

i) How can a parity check matrix $\mathbf{H}_S$ of the shortened code be obtained from the parity check matrix $\mathbf{H}$ of the original code? What are the dimensions of the parity check matrix $\mathbf{H}_S$ of the shortened code depending on N, K and M ?

Solution:

The parity check matrix of the shortened code $\mathbf{H}_S$ is obtained by deleting the first M rows in $\mathbf{H}$, which correspond to the deleted code bits. The resulting parity check matrix of the shortened code has dimension $N - M \times N - K$

j) Consider shortening of the $(7, 4, 3)_2$ Hamming code by $M = 3$. Determine the codewords of the resulting code. Which type of code is obtained?

Solution:

The codewords with $M = 3$ leading zeros from the table above are

$$\begin{array}{c} 000\ 0000 \\ 000\ 1111. \end{array}$$

In order to obtain the codewords of the shortened codes, the three leading zeros of the selected codewords have to be deleted. Hence, the resulting codewords are

$$\begin{array}{c} 0000 \\ 1111, \end{array}$$

belonging to a Rate $R = \frac{1}{4}$ repetition code.

6.9 Code Extension

Code extension refers to a method, where an overall parity check bit is added to each codeword of a given channel code. We denote the parity check matrix of the linear original code by $\mathbf{H}$. The parity check matrix $\mathbf{H}_e$ of the extended code can be obtained by adding first an all-zeros row and then an all-ones column to the original parity check matrix $\mathbf{H}$:

$$\mathbf{H}_e = \begin{bmatrix} & & & 1 \\ & \mathbf{H} & & \vdots \\ & & & 1 \\ 0 & \dots & 0 & 1 \end{bmatrix}$$

a) Is the code rate R_e of the extended code increased or decreased compared to the code rate R of the original code? Give reasons !

Solution:

For a block code which encodes K bits into N bit codewords, its code rate, R, is given as

$$R = \frac{K}{N}. \tag{6.6}$$

Consequently, the code rate of an extended code will be

$$R_e = \frac{K}{N+1}. \tag{6.7}$$

Thus, since $R_e < R$, the code rate is decreased.

b) Assume that the original code has an odd minimum Hamming weight $w_{\min}$. Determine the minimum Hamming distance $d_{\min,e}$ of the extended code depending on the minimum Hamming distance $d_{\min}$ of the original code.

Solution:

For linear block codes, the minimum Hamming distance is equal to the minimum hamming weight. The code word with minimum Hamming weight of the original code has an odd number of 1's. Therefore, the additional overall parity check bit in the extended code will be equal to 1 in this code word in order to make the checksum equal to zero. Therefore, the minimum Hamming weight and consequently the minimum Hamming distance will be increased by 1 compared to the original code. i.e.

$$d_{\min,e} = d_{\min} + 1. \tag{6.8}$$

c) Assume that the original code has an even minimum Hamming weight $w_{\min}$. Determine the minimum Hamming distance $d_{\min,e}$ of the extended code depending on the minimum Hamming distance $d_{\min}$ of the original code.

Solution:

For the same reasons explained in b), the additional overall parity check bit in the extended code will be equal to 0 in the code word having minimum Hamming weight. Therefore, the minimum Hamming weight and consequently the minimum Hamming distance will not be affected by code extension. i.e.

$$d_{\min,e} = d_{\min}. \tag{6.9}$$

d) Does code extension make sense regarding the error detection/error correction capabilities for codes with even or odd minimum Hamming distance, respectively? Give reasons!

Solution:

Error detection/correction capabilities of a code depend on its minimum Hamming distance. For a block code with odd minimum Hamming distance, code extension makes sense because it increases the minimum Hamming distance of the code. For a block code with even minimum Hamming distance, code extension does not make sense because it does not increase the minimum Hamming distance of the code.

For the remaining problems, we consider an original code with parity check matrix

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

e) Which type of code is defined by the parity check matrix $\mathbf{H}$.

Solution:

The parity check matrix defines a rate $R = \frac{1}{3}$ repetition code.

f) Determine a systematic generator matrix $\mathbf{G}$ for the original code.

Solution:

For a systematic linear block code with parity check matrix of the form

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}^T \\ \mathbf{I} \end{bmatrix} \tag{6.10}$$

(with $\mathbf{P}$ being the $(N-K) \times K$ parity submatrix, $(.)^T$ denotes the transpose operator and $\mathbf{I}$ is the $(N-K) \times (N-K)$ identy matrix), its generator matrix is given as

$$\mathbf{G} = \begin{bmatrix} \mathbf{I} \\ \mathbf{P} \end{bmatrix}. \tag{6.11}$$

From the given parity check matrix one identifies $\mathbf{P}^T$ as $\mathbf{P}^T = \begin{bmatrix} 1 & 1 \end{bmatrix}$. Hence,

$$\mathbf{G} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}. \tag{6.12}$$

g) Determine the minimum Hamming distance $d_{\min}$ of the original code.

Solution:

The minimum Hamming distance $d_{\min}$ of a rate $R = \frac{1}{3}$ repetition code is $d_{\min} = 3$.

h) Determine the parity check matrix $\mathbf{H}_e$ of the extended code.

Solution:

The extended code's parity check matrix will be

$$\mathbf{H}_e = \begin{bmatrix} & & & 1 \\ & \mathbf{H} & & \vdots \\ & & & 1 \\ 0 & \dots & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

i) Determine the set of code words of the extended code.

Solution:

The extended code is a rate $R = \frac{1}{4}$ repetition code whose codewords are

$$\mathbf{x}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T$$
$$\mathbf{x}_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}^T$$

j) Determine the minimum Hamming distance $d_{\min,e}$ of the extended code.

Solution:

Since the original code has an odd minimum Hamming distance,

$$\begin{aligned} d_{\min,e} &= d_{\min} + 1 \\ &= 3 + 1 \\ &= 4. \end{aligned}$$

Chapter 7

Low Density Parity Check Codes

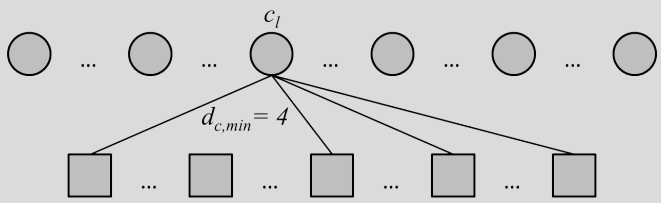
7.1 Minimum Hamming Distance of LDPC Codes

Consider an LDPC code which is represented by a parity check matrix $\mathbf{H}$. The minimum bit row weight of $\mathbf{H}$ is given by $d_{b,min}$. Let $c_l \in \{0, 1\}$ denote the code bit which is associated with the minimum row weight $d_{b,min}$. The girth of the Tanner graph is larger than 4.

a) By how many parity check equations is the code bit c_l checked?

Solution:

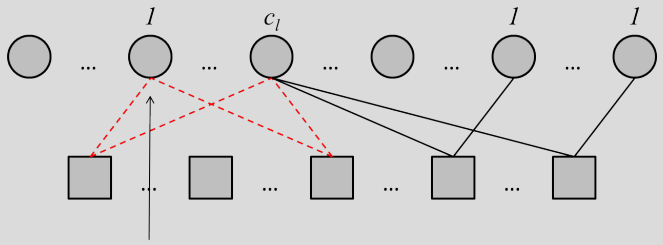
Each row of the parity check matrix $\mathbf{H}$ corresponds to a code bit and, therefore, to a bit node in the Tanner graph. The weight of the l-th row of $\mathbf{H}$ is equal to the degree of the bit node l and indicates the number of connected check nodes, i.e. by how many parity check equations the code bit c_l is checked. Therefore, the code bit c_l is checked by $d_{b,min}$ parity check equations.



b) Assume a codeword with $c_l = 1$. How many other non-zero code bits must be connected to each of the check nodes, to which c_l is connected? Can those non-zero code bits be the same for different check nodes?

Solution:

For a valid codeword, all parity check equations have to be met i.e. the modulo 2 sum of all connected node bits must be zero. Therefore, at least one other bit connected to each of the involved check nodes needs to be 1. These other bits have to be distinct bits for the different check nodes: If two of the other code bits are the same, a cycle of length 4 occurs (marked in red in the figure below). However, the girth (minimum cycle length) of the Tanner graph is larger than 4 (see task description).



c) Determine the minimum Hamming distance for the LDPC code with girth larger than 4 and minimum row weight $d_{b,min}$.

Solution:

LDPC codes are linear codes. The minimum Hamming distance is therefore equal to the minimum Hamming weight. According to task a), $d_{b,min}$ check nodes connected to c_l must at least be connected to $d_{b,min}$ other bit nodes which need to be 1 if $c_l = 1$. Thus each codeword has at least the weight $w_{H,min} = d_{b,min} + 1$.

Therefore, $d_{min} = w_{H,min} \geq d_{b,min} + 1$

d) What may be the consequence of increasing the minimum row weight $d_{b,min}$ in the design of LDPC codes with the purpose of increasing the minimum Hamming distance?

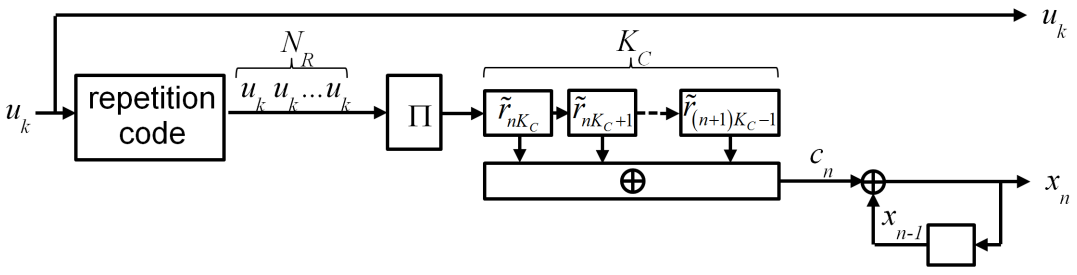
Solution:

Increasing the $d_{b,min}$ may result in a low code rate, since

$$R = 1 - \frac{\sum_i d_{b,i} \cdot i}{\sum_j d_{c,j} \cdot j}$$

7.2 Repeat Accumulate (RA) Code

The block diagram of a repeat accumulate (RA) code is depicted in the following figure:



The information bits and parity bits are denoted by $u_k \in 0, 1$ and $x_n \in 0, 1$, respectively. A parity check matrix of the RA-code is given by

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

a) Is the RA-code systematic? Give reasons!

Solution:

Yes, the information bits are an explicit part of the codewords.

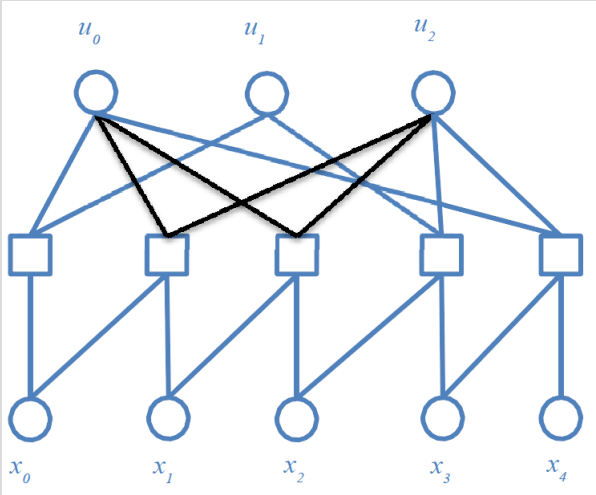
b) Is the RA-code regular or irregular? Give reasons!

Solution:

The RA-code is irregular. The columns of $\mathbf{H}^T$ representing the repetition and combiner part have different weight e.g. first column has weight 4 but second column has weight 2.

c) Sketch the Tanner graph which represents the parity check matrix $\mathbf{H}^T$ above.

Solution:



d) Determine the girth of the Tanner graph.

Solution:

The girth of the graph is 4.

e) Explain precisely why a short girth is undesired for message passing decoding.

Solution:

In message passing decoding, extrinsic information is exchanged along the edges of the Tanner graph. The nodes update the information based on all incoming information and the received channel information. The update rules assume that all incoming information and the channel information at a node are statistically independent. However, when the Tanner graph has cycles, the incoming information is not independent anymore after a few iterations resulting in a suboptimal decoding.

f) Mark a shortest cycle in the Tanner graph from c). Mark also the entries in the parity check matrix $\mathbf{H}^T$ which correspond to the marked cycle.

Solution:

The shortest cycle is marked in black in the answer to task c. The corresponding entries

are marked in the following parity check matrix:

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

g) Determine the rates R_R of the repetition coding part within the RA-code.

Solution:

The repetition code has an unequal rate for various input bits, i.e. $R_R = \frac{1}{4}$ for u_0 and u_2 but $R_R = \frac{1}{2}$ for u_1.

h) Determine the rate R_C of the combiner part within the RA-code.

Solution:

The rate of the combiner part is $R_C = 2$.

i) Determine the rate R_A of the accumulator part within the RA-code.

Solution:

The rate of the accumulator part is $R_A = 1$.

j) Determine the overall code rate R of the RA-code.

Solution:

The overall code rate R of the RA-code can be found from the parity check matrix or the Tanner graph as:

$$R = \frac{K}{N} = \frac{3}{3+5} = \frac{3}{8}$$

or from the following formula

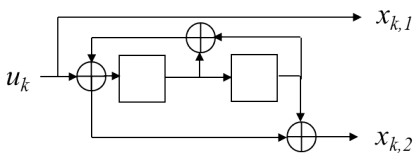
$$R = \frac{K}{K\left(1 + \frac{\bar{N}_R}{R_c}\right)} = \frac{3}{3+5} = \frac{3}{8}.$$

Using R_c from subtask h) and the average number of bits of the repetition code $\bar{N}_R = \frac{4+2+4}{3} = \frac{10}{3}$ (where the average number of bits $\bar{N}_R$ is used instead of N_R due to the fact that the repetition code is irregular) yields

$$R = \frac{1}{1 + \frac{10}{3 \cdot 2}} = \frac{6}{16} = \frac{3}{8}.$$

7.3 Tanner Graph of a Turbo Code

Consider the following encoder of a convolutional code



a) Is the convolutional encoder systematic ? Give reasons!

Solution:

Yes the convolutional encoder is systematic, since $x_{k,1} = u_{k,1}$

b) Determine the rate R of the convolutional code.

Solution:

$$R = \frac{K}{N} = \frac{1}{2}$$

c) Determine the code memory M.

Solution:

The memory is equal to the number of delay elements of the encoder.

$$M = 2$$

d) Determine the generator polynomials of the convolutional code.

Solution:

$$g_1(D) = 1$$
$$g_2(D) = \frac{1 + D^2}{1 + D + D^2}$$

e) Describe the generator polynomials in octal representation.

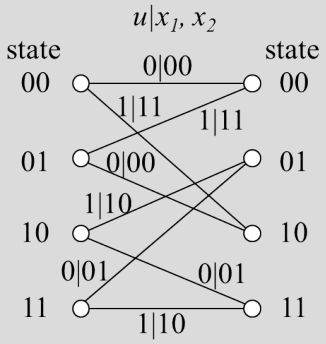
Solution:

$$g_1(D) = 1 + 0 \cdot D + 0 \cdot D^2 \qquad \Rightarrow 001_2 = 1_8$$
$$g_2(D) = \frac{1 + 0 \cdot D + D^2}{1 + D + D^2} \qquad \Rightarrow \frac{101_2 = 5_8}{111_2 = 7_8}$$

Thus, the octal representation of the generator polynomials is $(1, \frac{5}{7})$.

f) Sketch a trellis segment which describes the convolutional code. Label all nodes and transitions completely.

Solution:



g) Determine for all states of the convolutional encoder the information bit sequence, which has to be fed into the encoder in order to terminate the code in the all zero state.

Solution:

state	termination sequence	
s_k	u_{k+1}	u_{k+2}
00	0	0
01	1	0
10	1	1
11	0	1

For the remaining problems, consider that the information bit sequence

$$u_0, u_1, u_2, u_3, u_4$$

of the length $K = 5$ is encoded without termination. The encoder is initialized in the all-zeros-state.

h) Determine the sequence of encoder states depending on $u_0, ..., u_4$ for the complete encoding process.

Solution:

u_k	s_k	
u_0	0	0
u_1	u_0	0
u_2	$u_0 \oplus u_1$	u_0
u_3	$u_0 \oplus u_1 \oplus u_0 \oplus u_2$	$u_0 \oplus u_1$
	$= u_1 \oplus u_2$	
u_4	$u_0 \oplus u_1 \oplus u_1 \oplus u_2 \oplus u_3$	$u_1 \oplus u_2$
	$= u_0 \oplus u_2 \oplus u_3$	

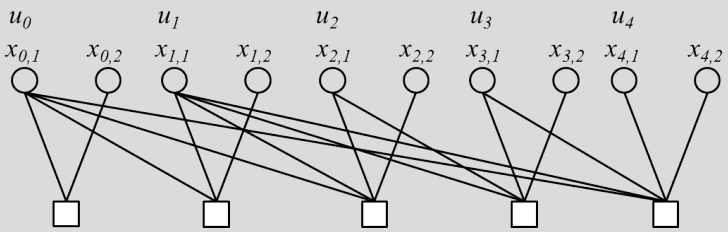
i) Determine the parity bit sequence $x_{0,2}, x_{1,2}, x_{2,2}, x_{3,2}, x_{4,2}$ depending on $u_0, ..., u_4$.

Solution:

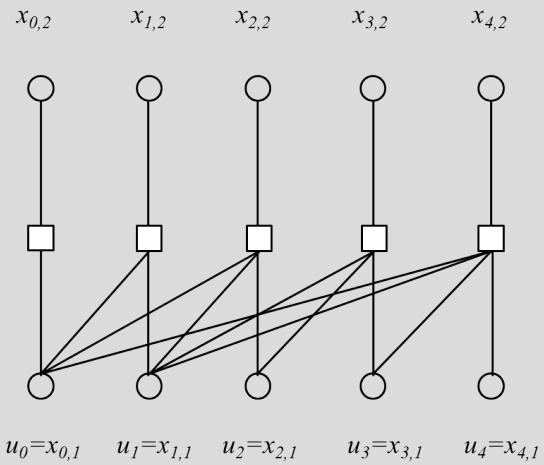
$$
\begin{aligned}
x_{k,1} &= u_k, \quad \forall k \\
x_{0,2} &= u_0 \\
x_{1,2} &= u_0 \oplus u_1 \\
x_{2,2} &= u_0 \oplus u_0 \oplus u_1 \oplus u_2 \oplus u_0 = u_0 \oplus u_1 \oplus u_2 \\
x_{3,2} &= u_0 \oplus u_1 \oplus u_1 \oplus u_2 \oplus u_3 + u_0 \oplus u_1 = u_1 \oplus u_2 \oplus u_3 \\
x_{4,2} &= u_1 \oplus u_2 + u_0 \oplus u_1 \oplus u_3 \oplus u_4 + u_1 \oplus u_2 = u_0 \oplus u_1 \oplus u_3 \oplus u_4
\end{aligned}
$$

j) Sketch the Tanner graph of the convolutional code. Label the bit nodes!

Solution:



Reordering the nodes yields a clearer view on the graph:



k) Is message passing a suitable decoding method for the convolutional code? Give reasons!

Solution:

- Tanner graph has short cycles of length 4.
- Tanner graph is not sparse.
- Parity bits $x_{k,2}, \quad \forall k$ are connected to only one check node.

$\Rightarrow$ The convolutional code is not suitable for message passing decoding.

l) Determine the parity check matrix $\mathbf{H}^T$ of the convolutional code for an information word length $K = 5$.

Solution:

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

For the remaining problems, consider a rate $R = 1/3$ turbo encoder which uses the recursive convolutional code above as constituent codes and an interleaver which is determined by the permutation matrix

$$\mathbf{\Pi} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \text{i.e.} \qquad \begin{bmatrix} \tilde{u}_0 \\ \tilde{u}_1 \\ \tilde{u}_2 \\ \tilde{u}_3 \\ \tilde{u}_4 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}}_{\mathbf{\Pi}} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix},$$

where $\tilde{\mathbf{u}} = [\tilde{u}_0, ..., \tilde{u}_4]^T$ denotes the interleaved information bit sequence.

m) Determine the sequence of interleaved bits depending on $u_0, ..., u_4$

Solution:

$$\begin{aligned} \tilde{u}_0 &= u_0 \\ \tilde{u}_1 &= u_3 \\ \tilde{u}_2 &= u_1 \\ \tilde{u}_3 &= u_4 \\ \tilde{u}_4 &= u_2 \end{aligned}$$

n) Determine the permutation matrix of the deinterleaver.

Solution:

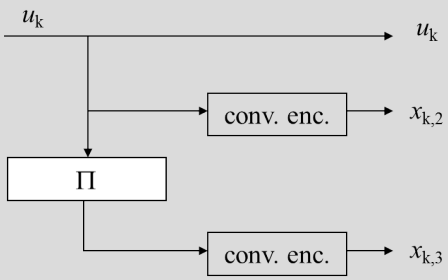
$$\mathbf{\Pi}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The product of the permutation matrix of the deinterleaver with the vector of interleaved bits has to yield the bits in original order:

$$\mathbf{\Pi}^{-1} \cdot \tilde{\mathbf{u}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} u_0 \\ u_3 \\ u_1 \\ u_4 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix}$$

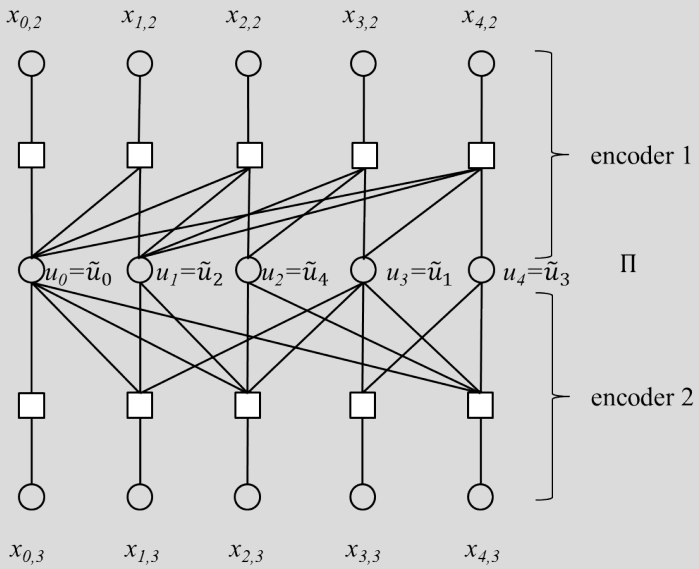
o) Sketch the block diagram of the turbo encoder.

Solution:



p) Sketch the Tanner graph which represents the turbo code.

Solution:



q) Will message passing perform well for the given turbo code? Give reasons.

Solution:

Message passing will not perform well, since

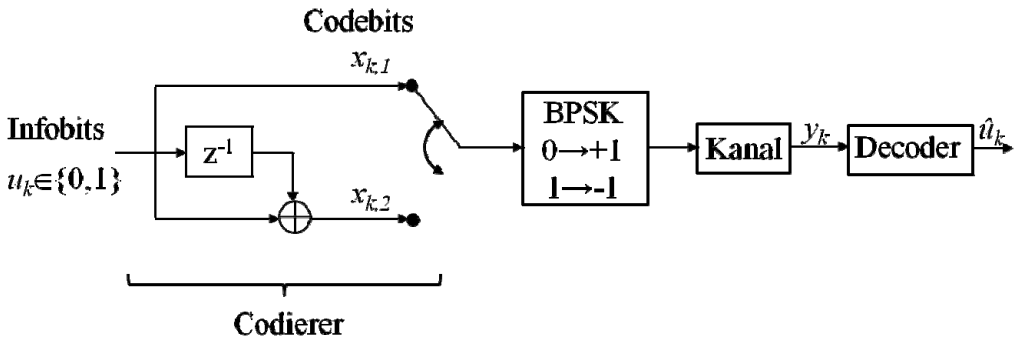
- Tanner graph has short cycles
- parity bits $x_{k,2}$ and $x_{k,3}$, $\forall k$ are connected to only one check node.

Chapter 8

Convolutional Code

8.1

The encoder of a convolutional code is given in the following figure. (This code shall be used in all parts of the problem except for part d).)



At the beginning the encoder is in state "0", i.e. the memory element is initialized with "0". The convolutional code is terminated in state "0".

a) Is the encoder systematic? Explain your answer!

Solution:

The code is systematic, because the code bit $x_{k,1}$ is equal to to information bit u_k.

b) What is the code rate R of the convolutional code?

Solution:

For each input bit two output bits are generated:

$$R = \frac{1}{2}$$

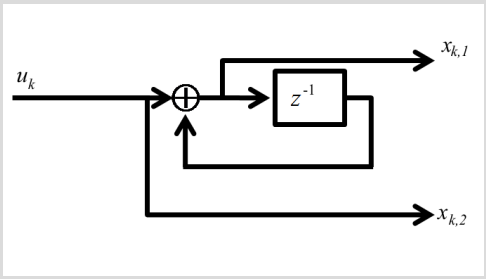
c) Determine the generator polynomials $g_n(D)$ of the encoder?

Solution:

$$g_1(D) = 1$$
$$g_2(D) = 1 + D$$

d) Determine the generator polynomials of a recursive encoder, which generates the same code. Sketch the recursive encoder.

$$g_1(D) = \frac{1}{1+D}$$
$$g_2(D) = 1$$

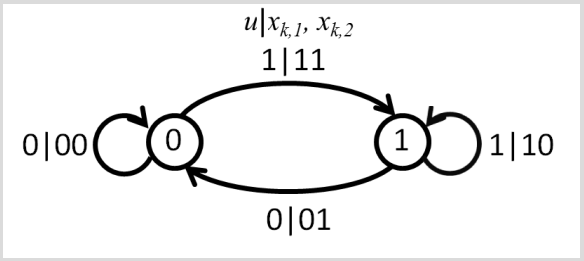


e) How many information bits are necessary to terminate the code in a certain state?

$M = 1$ bit is necessary to terminate the code.

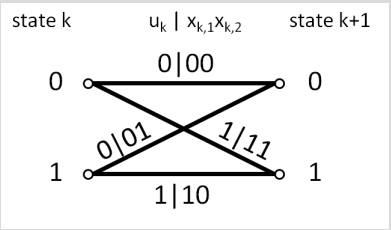
f) Sketch the state diagram of the convolutional code. Label the diagram clearly and completely.

The state diagram is:

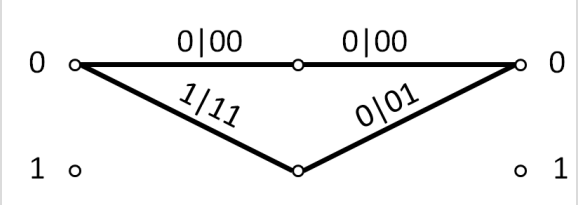


g) Sketch a trellis-segment with all possible transitions. Label the diagram clearly and completely.

The trellis is:



h) Determine the free distance d_f of the code.



$d_f = d_H(\begin{bmatrix}1 & 1 & 0 & 1\end{bmatrix}^T, \begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}^T) = 3$. The free distance is $d_f = 3$.

i) Determine the maximum length of an error burst, which allows error-free decoding with hard decision decoding.

$t \leq \left\lfloor \frac{d_f - 1}{2} \right\rfloor$ bit $= \frac{3-1}{2}$ bit $= 1$ bit

j) Consider an information word of length 2 bit, i.e. $\mathbf{u} = \begin{bmatrix} u_1 & u_2 \end{bmatrix}^T$. (Note: Consider that the code is terminated in state "0"!)

(1) State all possible codewords $\mathbf{x}$ and assign them in a table to the corresponding information words $\mathbf{u} = \begin{bmatrix} u_1 & u_2 \end{bmatrix}^T$.

u_1	u_2	termination	$\mathbf{x}$			
0	0	0	00	00	00	$= \mathbf{x}_1$
0	1	0	00	11	01	$= \mathbf{x}_2$
1	0	0	11	01	00	$= \mathbf{x}_3$
1	1	0	11	10	01	$= \mathbf{x}_4$

(2) Is the code linear? Explain your answer!

$$\begin{aligned} \mathbf{x}_2 + \mathbf{x}_3 &= \mathbf{x}_4 \\ \mathbf{x}_2 + \mathbf{x}_4 &= \mathbf{x}_3 \\ \mathbf{x}_3 + \mathbf{x}_4 &= \mathbf{x}_2 \\ \mathbf{x}_i + \mathbf{x}_i &= \mathbf{0} = \mathbf{x}_1 \\ \mathbf{x}_i + \mathbf{x}_1 &= \mathbf{x}_i + \mathbf{0} = \mathbf{x}_i \end{aligned}$$

The mod-2 sum of any two codewords is also a codeword.
$\Rightarrow$ The code is linear.

(3) Determine a generator matrix $\mathbf{G}$ of a block code, that generates the same code.

Solution:

$$\mathbf{x} = \mathbf{G}\mathbf{u}$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

(4) Determine the code rate R_B of the block code?

$$R_B = \frac{K}{N} = \frac{2}{6} = \frac{1}{3}$$

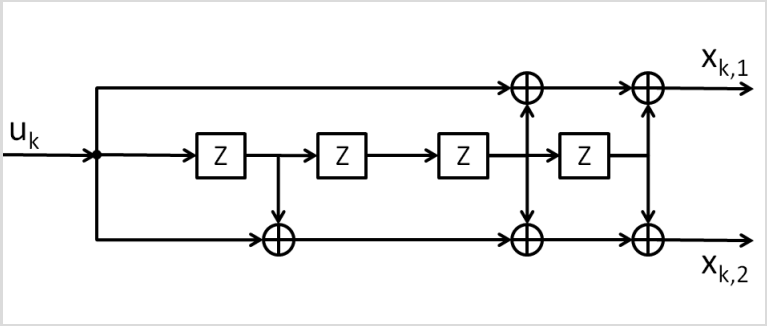
8.2 Convolutional Code of the GSM-mobile System

For the transmission of speech, the GSM system uses a binary convolutional code with the following generator polynomials:

$$\begin{aligned} g_1(D) &= 1 + D^3 + D^4 \\ g_2(D) &= 1 + D + D^3 + D^4 \end{aligned}$$

a) Sketch the encoder (shift register).

The encoder is shown in the following picture.



b) Determine the memory M and the constraint length C of the convolutional code.

$$M = 4$$
$$C = M + 1 = 5$$

c) Determine the code rate R of the convolutional code.

Solution:

For each input bit two output bits are generated:

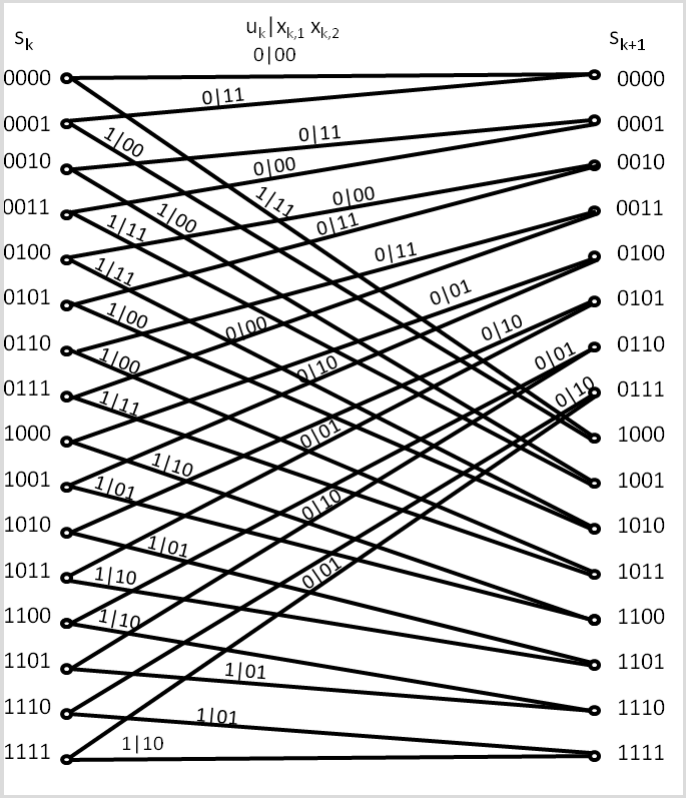
$$R = \frac{1}{2}$$

d) Is the encoder systematic? Explain your answer!

A convolutional encoder is systematic, if either $x_{k,1} = u_k$ or $x_{k,2} = u_k$. This corresponds to $g_1(D) = 1$ or $g_2(D) = 1$

As this is not the case here, the encoder is not systematic.

e) Sketch a trellis segment with all possible transitions. Label the figure completely! In particular, define the states of the trellis and the variables which determine the transitions clearly.



f) Determine the metric increment of a Viterbi decoder with soft-decision maximum-likelihood (ML)-decoding for an AWGN-channel.

Solution:

$$\begin{aligned}
\max_{\mathbf{x}} p(\mathbf{y}|\mathbf{x}) &= \max_{\mathbf{x}} \prod_{k=1}^{L} \prod_{n=1}^{N} p(y_{k,n}|x_{k,n}) \\
&= \max_{\mathbf{x}} \sum_{k=1}^{L} \sum_{n=1}^{N} \log p(y_{k,n}|x_{k,n}) \\
&= \max_{\mathbf{x}} \left\{ \sum_{l=1}^{k-1} \sum_{n=1}^{N} \log p(y_{l,n}|x_{l,n}) + \underbrace{\sum_{n=1}^{N} \log p(y_{k,n}|x_{k,n})}_{\Delta\mu_k(s_i,s_j)} + \sum_{t=k+1}^{L} \sum_{n=1}^{N} \log p(y_{t,n}|x_{t,n}) \right\}
\end{aligned}$$

$$\begin{aligned}
\log p(y_{k,n}|x_{k,n}) &= \log \frac{1}{\sqrt{2\pi\sigma_n^2}} - \frac{(y_{k,n} - x_{k,n})^2}{2\sigma_n^2} \\
&= \underbrace{\log \frac{1}{\sqrt{2\pi\sigma_n^2}}}_{const.} - \frac{1}{2\sigma_n^2} \left(\underbrace{y_{k,n}^2}_{const.} - 2y_{k,n}x_{k,n} + x_{k,n}^2 \right)
\end{aligned}$$

For $x_{k,n} \in \{0,\ 1\}$:

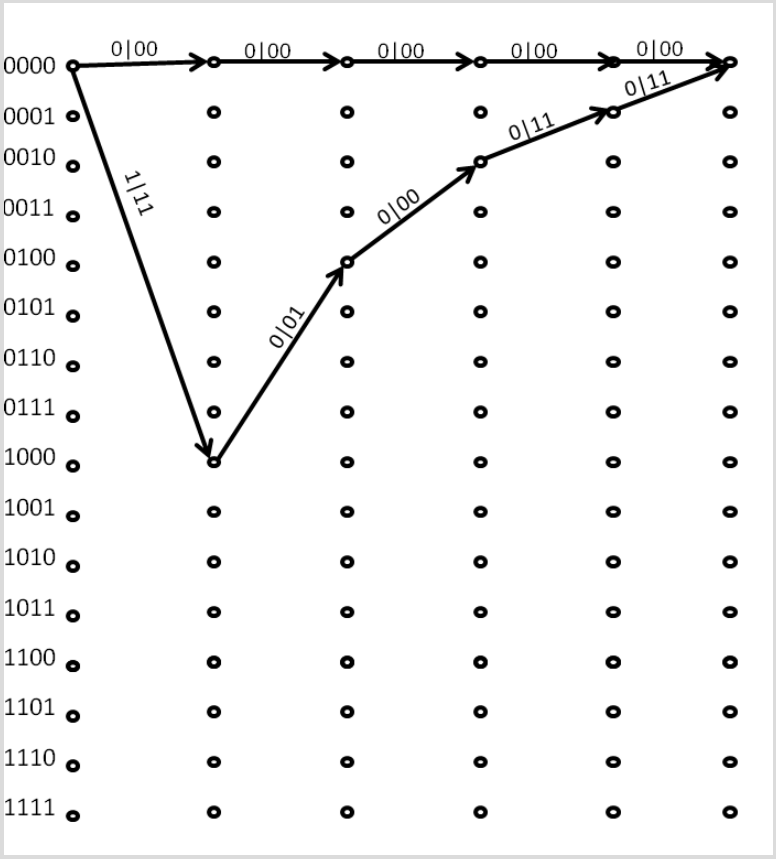
$$\Delta\mu_k(s_i, s_j) = \sum_{n=1}^{2} y_{k,n}x_{k,n}(s_i, s_j) - \frac{1}{2}x_{k,n}^2(s_i, s_j)$$

For $x_{k,n} \in \{\pm 1\}$

$$\Delta\mu_k(s_i, s_j) = \sum_{n=1}^{2} y_{k,n} x_{k,n}(s_i, s_j)$$

g) Determine the free distance d_f of the code.

Solution:



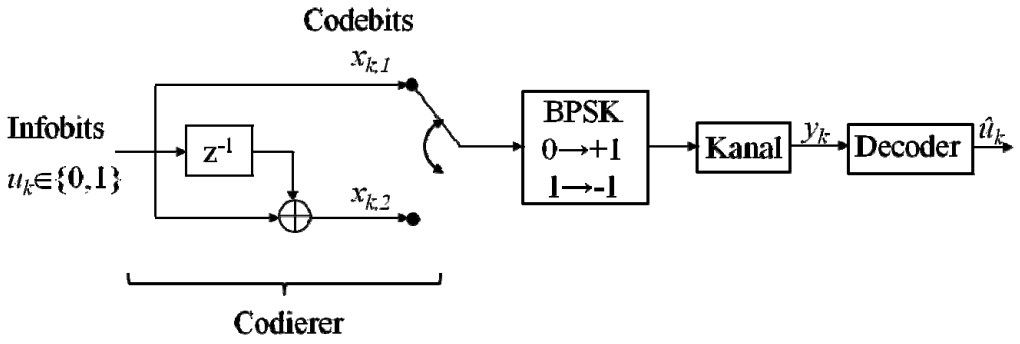
Compare the $\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}^T$ and $\begin{bmatrix}1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1\end{bmatrix}^T$.

$\Rightarrow$ The free distance is $d_f = 7$.

The free distance is the minimum Hamming weight among all possible code sequences. We have to search for a sequence, which diverges from the all-zero sequence and remerges with the all-zero sequence with the minimum number of codebits equal "1".

8.3

Consider the convolutional code, which is determined by the following picture.



The encoder is initialized in state "0", i.e. all memory elements contain "0". The convolutional code will be terminated in state "0".

a) State the generator polynomials $g_n(D)$ of the encoder.

Solution:

$$g_1(D) = 1$$
$$g_2(D) = 1 + D$$

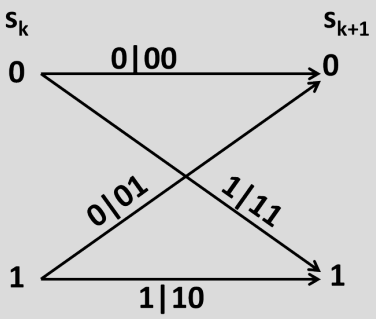
b) Describe the generator polynomials of the encoder in octal representation.

Solution:

$$g_1(D) = \underbrace{\begin{matrix} 0 & + & 1 & + & 0 \cdot D \\ 0 & & 1 & & 0 \end{matrix}}_{2_8}$$
$$g_2(D) = \underbrace{\begin{matrix} 0 & + & 1 & + & 1 \cdot D \\ 0 & & 1 & & 1 \end{matrix}}_{3_8}$$

c) Sketch a trellis segment with all possible transitions. Label the figure completely.

Solution:



d) For an AWGN-channel with noise variance σ_N^2, derive the expression for the metric increment of a Viterbi-decoder with

(1) soft-decision MAP-decoding

(2) soft-decision maximum-likelihood decoding

using log-likelihood ratios (L-values). Assume that the code bits $\mathbf{x_k}$ are transmitted with BPSK-modulation, i.e. $x_k \in \{\pm 1\}$.

Solution:

(1) For MAP decoding, we need to find the code sequence $\hat{\mathbf{x}}$ which maximizes the a posteriori probabilities $p(\mathbf{x}|\mathbf{y})$

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} p(\mathbf{x}|\mathbf{y})$$

Since the channel is memoryless, this can be rewritten as

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} \prod_{l=1}^{L} \prod_{n=1}^{N} p(x_{l,n}|y_{l,n})$$

where L ist the number of trellis segments and $N = 2$ is the number of codebits per trellis segment.

Taking the logarithm of the probabilities does not change the result of the maximization. Hence, we have

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} \sum_{l=1}^{L} \sum_{n=1}^{N} \log p(x_{l,n}|y_{l,n}).$$

We divide the sum for l ind already processed segmetns $l < k$, the currently processed segment $l = k$ and the future segments $l > k$:

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} \left\{ \sum_{l=1}^{k-1} \sum_{n=1}^{N} \log p(x_{l,n}|y_{l,n}) + \underbrace{\sum_{n=1}^{N} \log p(x_{k,n}|y_{k,n})}_{\Delta\mu_k(s_i,s_j)} + \sum_{l=k+1}^{L} \sum_{n=1}^{N} \log p(x_{l,n}|y_{l,n}) \right\}.$$

This representation indicates, that the metric which is to be maximized can be successively calculated by adding a metric increment

$$\Delta\mu_k(s_i, s_j) = \sum_{n=1}^{N} \log p(x_{k,n}|y_{k,n})$$

for each trellis segment. This metric increment has to be computed for each trellis transition from state s_i to state s_j.

In this calculation, we have to insert the codebits $x_{k,n}$ which are associated with the trellis transition from state s_i to state s_j.

Using Bayes' rule, the metric increment can be reformulated as

$$\begin{aligned}\Delta\mu_k(s_i, s_j) &= \sum_{n=1}^{N} \log \frac{p(y_{k,n}|x_{k,n})p(x_{k,n})}{p(y_{k,n})} \\ &= \sum_{n=1}^{N} \log p(y_{k,n}|x_{k,n}) + \sum_{n=1}^{N} \log p(x_{k,n}) - \sum_{n=1}^{N} \log p(y_{k,n}).\end{aligned}$$

The first term is the channel transition probability $p(y_{k,n}|x_{k,n})$ which is known from the channel model.

As $x_{k,n}$ labels a trellis transition, the second term $\sum_{n=1}^{N} \log p(x_{k,n})$ can be interpreted as the probability $p(s_j|s_i)$ that in the k-th segment, the trellis will change to state s_j given that the previous state was state s_i.

This state transition is caused by the particular information bit u_k which labels the trellis transition. Therefore, we can replace the second term in the equation above by

$$\sum_{n=1}^{N} \log p(x_{k,n}) = \log p(s_j|s_i) = \log p(u_k).$$

$p(u_k)$ is the a priori information, which might be known from the source statistics.

The last term $\sum_{n=1}^{N} \log p(y_{k,n})$ is independent of the tested codeword $\mathbf{x}$ and, therefore, changes the metric increment of all paths by the same additive value. Since adding the same value to all candidate paths does not change the result of the metric maximization, the third term can be dropped.

The metric increment then becomes

$$\Delta\mu_k = \left[\sum_{n=1}^{N} \log p(y_{k,n}|x_{k,n})\right] + \log p(u_k). \tag{8.1}$$

We now express $\log p(u_k)$ by the a priori log-likelihood ratio

$$\begin{aligned} L_a(u_n) &= \log \frac{p(u_n = +1)}{p(u_n = -1)} \\ \Rightarrow p(u_k) &= \underbrace{\frac{e^{\frac{L_a(u_k)}{2}}}{1 + e^{L_a(u_k)}}}_{\text{const}} e^{\frac{u_k L_a(u_k)}{2}} \\ \Rightarrow \log p(u_k) &= \log(\text{const}) + \frac{1}{2} u_k L_a(u_k) \end{aligned} \tag{8.2}$$

The constant can again be dropped as it does not have an impact on the result of the metric maximization.

Similarly, we express the channel information by the log-likelihood ratio

$$\begin{aligned} L_c(x_{k,n}) &= \log \frac{p(y_{k,n}|x_{k,n} = +1)}{p(y_{k,n}|x_{k,n} = -1)} \\ \Rightarrow p(y_{k,n}|x_{k,n}) &= \text{const} \cdot e^{\frac{x_{k,n} L_x(x_{k,n})}{2}} \\ \Rightarrow \log p(y_{k,n}|x_{k,n}) &= \log(\text{const}) + \frac{1}{2} x_{k,n} L_c(x_{k,n}) \end{aligned} \tag{8.3}$$

Using (8.2) and (8.3), the metric increment (8.1) becomes

$$\Delta\mu_k(s_i, s_j) = \left[\sum_{n=1}^{N} \frac{1}{2} x_{k,n} L_c(x_{k,n})\right] + \frac{1}{2} u_k L_a(u_k).$$

Finally, we can determine the channel info $L_c(x_{k,n})$ for an AWGN channel:

$$\begin{aligned}
L_c(x_{k,n}) &= L(y_{k,n}|x_{k,n}) \\
&= \log \frac{p(y_{k,n}|x_{k,n}=1)}{p(y_{k,n}|x_{k,n}=-1)} \\
&= \log \frac{\frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y_{k,n}-1)^2}{2\sigma_N^2}}}{\frac{1}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{(y_{k,n}+1)^2}{2\sigma_N^2}}} \\
&= -\frac{(y_{k,n}-1)^2}{2\sigma_N^2} + \frac{(y_{k,n}+1)^2}{2\sigma_N^2} \\
&= \frac{1}{2\sigma_N^2}[-y_{k,n}^2 + 2y_{k,n} - 1 + y_{k,n}^2 + 2y_{k,n} + 1] \\
&= \frac{1}{2\sigma_N^2} 4y_{k,n} \\
&= \frac{2}{\sigma_N^2} y_{k,n}.
\end{aligned}$$

The metric increment for MAP decoding can then be written as

$$\Delta\mu_k(s_i, s_j) = \frac{1}{\sigma_N^2} \sum_{n=1}^{N} x_{k,n} y_{k,n} + \frac{1}{2} u_k L_a(u_k).$$

Note, that the MAP decoder requires knowledge of the noise variance σ_N^2 as weighting factor between channel information and a priori information.

(2) For ML decoding, the a priori information $L_a(u_k)$ is not taken into account. Instead a uniform source symbol distribution is assumed, i.e.

$$L_a(u_n) = \log \frac{p(u_n=+1)}{p(u_n=-1)} = \log \frac{\frac{1}{2}}{\frac{1}{2}} = 0.$$

The metric increment then simplifies to

$$\Delta\mu_k(s_i, s_j) = \frac{1}{\sigma_N^2} \sum_{n=1}^{N} x_{k,n} y_{k,n}.$$

The noise variance is now only a scaling factor which is the same for all candidate paths and all trellis segments. Hence, the precise value of σ_N^2 has no impact on the result of the metric maximization and can be set to $\sigma_N^2 = 1$, i.e.

$$\Delta\mu_k(s_i, s_j) = \sum_{n=1}^{N} x_{k,n} y_{k,n}.$$

Note, that unlike the MAP decoder, the ML decoder does not require knowledge of the noise variance σ_N^2.

e) At the input of the decoder, the sequence

$$\mathbf{y} = \begin{bmatrix} +0.5 & -2.0 & -1.0 & +1.5 \end{bmatrix}^T$$

is observed.

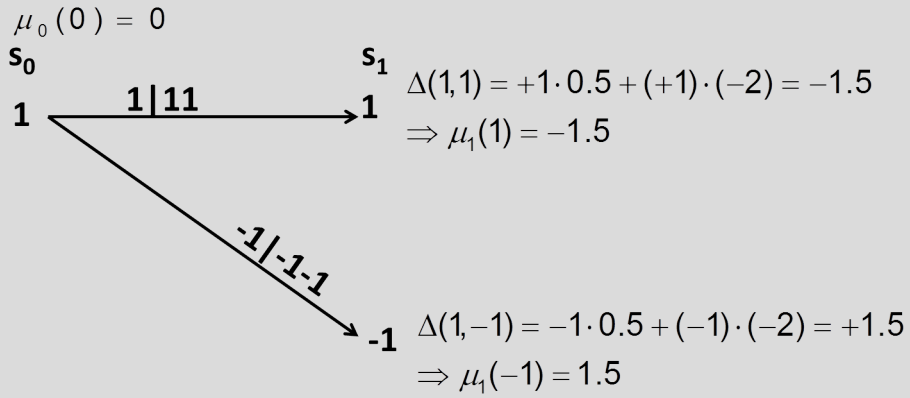
Performe the Viterbi-algorithm for Soft-Decision Maximum-Likelihood decoding and determine the decoded information sequence. Make sure that all steps are clearly explained.

Solution:

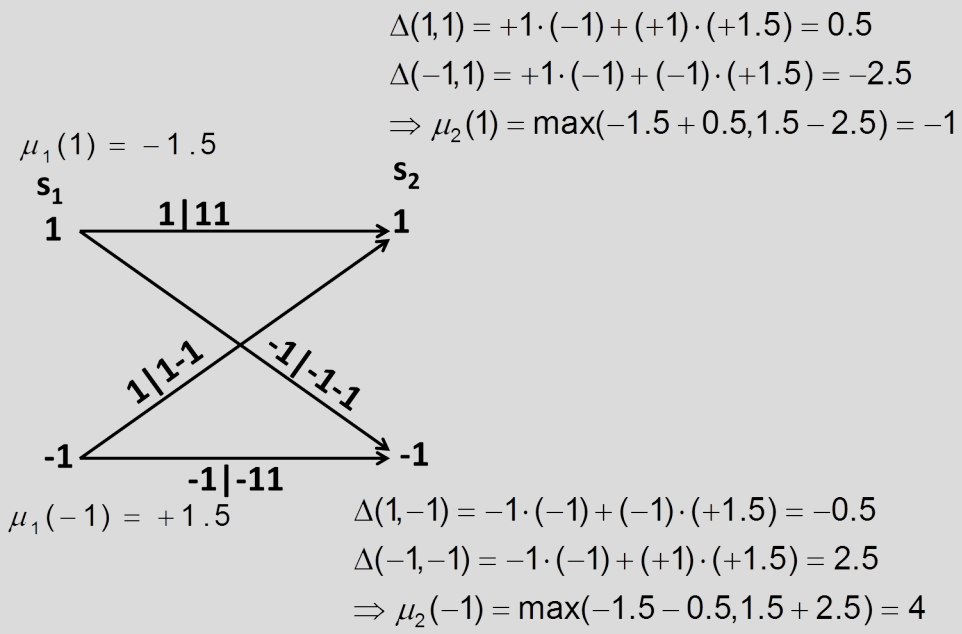
The encoder was initialized in the zero state. As we consider BPSK modulation, the

decoder trellis starts from state +1.

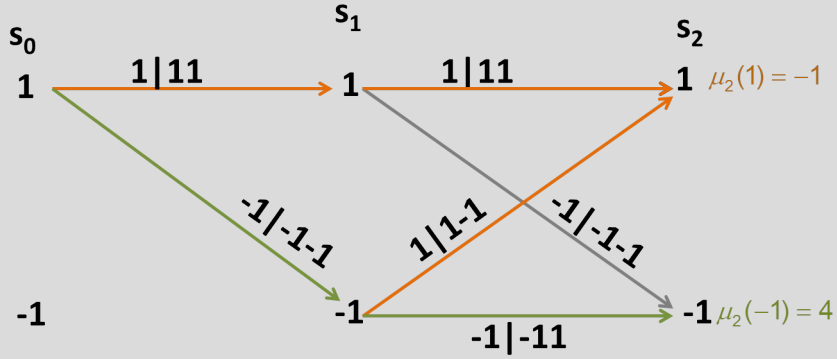
The observed samples $y_{1,1} = 0.5$ and $y_{1,2} = -2.0$ correspond to the first trellis segment. Hence, the metric increments $\Delta(s_0, s_1)$ and the metric $\mu_1(s_1)$ are obtained as indicated in the following figure.



In the next trellis segment $y_{2,1} = -1.0$ and $y_{2,2} = +1.5$ is received. Then, the metrics $\mu_2(s_2)$ are:



As $\mu_2(-1) = 4 > \mu_2(1) = -1$, the path ending in state "-1" (green),is more likely than the path ending in state "1" (orange).

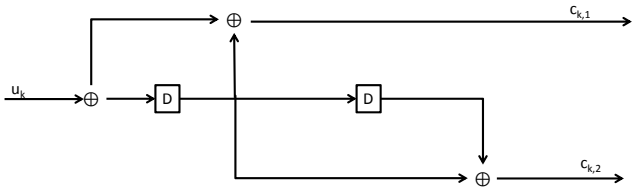


Therefore, the the ML codeword is $\hat{\mathbf{x}} = \begin{bmatrix} -1 & -1 & -1 & +1 \end{bmatrix}^T$ and the decoded information word $\hat{\mathbf{u}} = \begin{bmatrix} -1 & -1 \end{bmatrix}^T$.

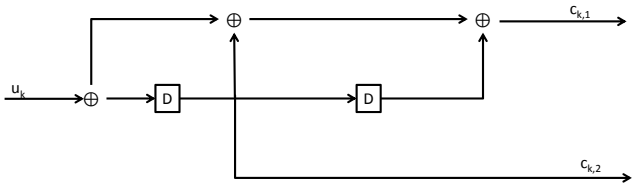
8.4

Consider the following three different shift registers.

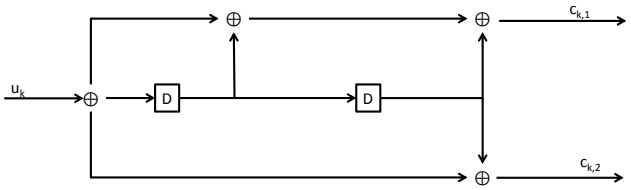
1)



2)



3)



a) Determine the generator polynomials of the convolutional encoder 1) and 2)?

Solution:

convolutional encoder 1):

$$g_1^{(1)}(D) = 1 + D$$
$$g_2^{(1)}(D) = D + D^2$$

convolutional encoder 2):

$$g_1^{(2)}(D) = 1 + D + D^2$$
$$g_2^{(2)}(D) = D$$

b) Are the shift register 1) and 2) catastrophic encoders? Explain your answer! What is the major problem of catastrophic encoders?

Solution:

A convolutional encoder is non-catastrophic, if the generator polynomials $g_n(D)$ do not have common factors. As $g_2^{(1)}(D) = D + D^2 = D(1+D) = D \cdot g_1^{(1)}(D)$ the convolutional code 1) is catastrophic.

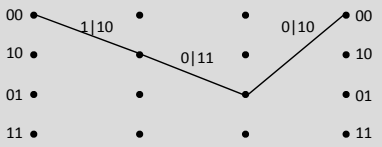
As $g_2^{(2)}(D)$ contains only the root 0, but 0 is no root of $g_1^{(2)}(D)$, it holds that the largest common divisor of $g_1^{(2)}(D)$ and $g_2^{(2)}(D)$ is 1. The convolutional code 2) is not catastrophic.

The disadvantage of catastrophic convolutional codes is, that an information sequence with infinite weight can generate a code sequence with finite weight. Hence, a small number of erroneous code bits can cause an infinite error sequence.

c) Determine the free distance of the convolutional codes 2) and 3)!

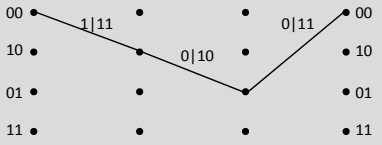
Solution:

Convolutional code 2:



$$d_f^{(2)} = d_H\left(\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}^T, \begin{bmatrix}1 & 0 & 1 & 1 & 1 & 0\end{bmatrix}^T\right) = 4$$

Convolutional code 3:



$$d_f^{(3)} = d_H\left(\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}^T, \begin{bmatrix}1 & 1 & 1 & 0 & 1 & 1\end{bmatrix}^T\right) = 5$$

d) Which of the shift registers 2) or 3) would you prefer? Explain your answer!

Solution:

Register 3) is preferable as it produces a code with larger free distance.

e) What is the rate R_3 of the convolutional code 3)?

Solution:

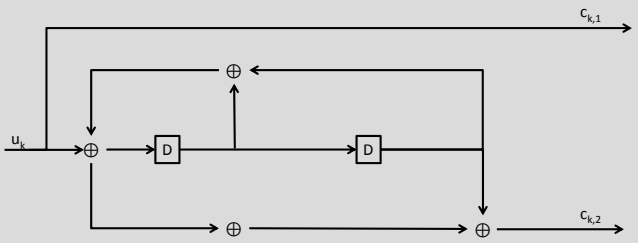
$$R_3 = \frac{\text{input bits per time step}}{\text{output bits per time step}} = \frac{1}{2}$$

f) Determine the constraint length C_3 and the memory M_3 of the convolutional code 3)?

Solution:

$C^{(3)} = 3$ (number of memory elements + 1)
$M^{(3)} = 2$ (number of memory elements)

g) Sketch the shift register of the equivalent recursive convolutional encoder, that generates the same code as the shift register 3).



h) State the expression for the metric increment of a Viterbi-decoder with soft-decision maximum-likelihood decoding (ML) decoding for an AWGN channel.

For $x_{k,n} \in \{0, 1\}$:

$$\Delta\mu_k(s_i, s_j) = \left(\sum_{n=1}^{2} y_{k,n} x_{k,n}(s_i, s_j)\right) - \frac{1}{2} x_{k,n}^2(s_i, s_j)$$

For $x_{k,n} \in \{\pm 1\}$:

$$\Delta\mu_k(s_i, s_j) = \sum_{n=1}^{2} y_{k,n} x_{k,n}(s_i, s_j)$$

8.5

Consider the following generator polynomials of a convolutional code:

$$g_1(D) = 1 + D + D^2 + D^3$$
$$g_2(D) = 1 + D + D^3$$

a) Determine the code rate R.

Solution:

For each input bit the two polynomials generate two output bits:

$$R = \frac{1}{2}$$

b) Determine the memory M and the constraint length C of the convolutional code.

Solution:

The largest exponent of the polynomials defines the number of required memory elements $M = 3$.

$$C = M + 1 = 4$$

c) Determine the octal representation of the convolutional code.

Solution:

$$\begin{array}{rcccccccc} g_1(D) & = & & & & 1 & +D & +D^2 & +D^3 \\ & & 0 & 0 & 1 & 1 & 1 & 1 & \\ & & \underbrace{\qquad\qquad}_{1_8} & & & \underbrace{\qquad\qquad\qquad\qquad}_{7_8} & & & \end{array}$$

and

$$g_2(D) = \underbrace{0\ 0\ 1}_{1_8} \quad \underbrace{1 + D + 0 + D^3}_{5_8}$$

$\Rightarrow$ The octal representation is 17_8 for $g_1(D)$ and 15_8 for $g_2(D)$.

d) Determine an upper bound on the free distance d_f using the generator polynomials.

Solution:

$$d_f \leq \sum_{n=1}^{N} w_H(g_n(D)) = 4 + 3 = 7$$

e) Check if the encoder is catastrophic or not. What characterizes a catastrophic encoder?

Solution:

$$g_1(D) : g_2(D) = (D^3 + D^2 + D + 1) : (D^3 + D + 1) = 1 + \frac{D^2}{D^3 + D + 1}$$

$\Rightarrow$ $g_1(D)$ is not a multiple of $g_2(D)$.

Additional it holds, that $g_2(1) = 1 \mod 2$ and that $g_2(0) = 1 \mod 2$. $g_2(D)$ has no root modulo 2 and therefore no divisor of degree 1. $g_2(D)$ is not a product of two polynomial with lower degree, as one of those would have to have degree 1. Therefore, $g_2(D)$ has no common divisor with $g_1(D)$ of degree 1 or 2.

$\Rightarrow$ The generator polynomials $g_1(D)$ and $g_2(D)$ have no common divisor.

$\Rightarrow$ The encoder is non catastrophic.

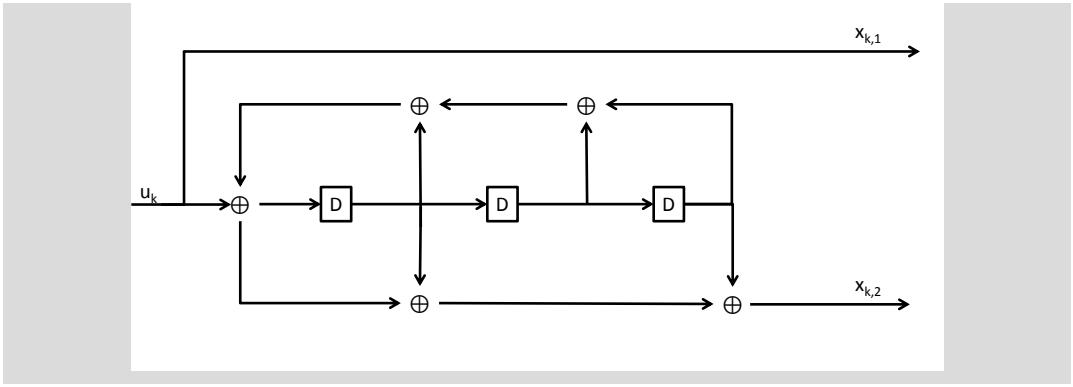
A catastrophic encoder is characterized by the fact, that an information sequence with infinite weight produces a code sequence of low (finite) weight. Hence, a small number of erroneous code bits can cause an infinite error sequence.

f) Determine the generator polynomials of a recursive systematic encoder, that generates the same code. $g_1(D)$ is supposed to define the feedback.

$$g_{RS,1} = \frac{g_1(D)}{g_1(D)} = 1$$
$$g_{RS,2} = \frac{g_2(D)}{g_1(D)} = \frac{1 + D + D^3}{1 + D + D^2 + D^3}$$

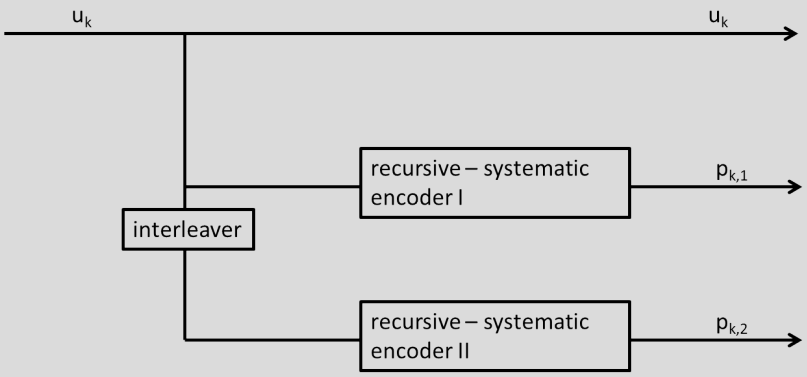
g) Sketch the recursive-systematic encoder of part f) as a shift register.

Solution:



h) Sketch the encoder of a Turbo-Code, that uses recursive-systematic convolutional codes as component codes.

Solution:



i) Which fundamental difference between a recursive and a non-recursive convolutional code explains why recursive-systematic convolutional codes are particularly suitable for Turbo-Codes? Give an explanation.

Solution:

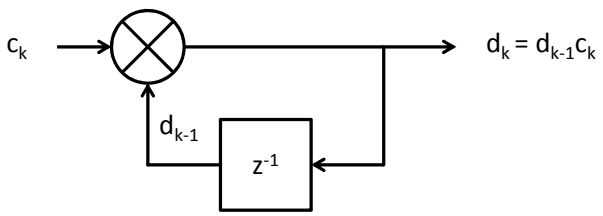
The recursive systematic encoder generates an infinite impulse response (IIR). The non recursive encoder has a finite impulse response of length $C = M + 1$.

If non-recursive convolutional codes are used as constituent codes of a turbo code, an information sequence with low hamming weight will result in code sequences of low Hamming weight for both constituent codes. Therefore, the Hamming weight of the overall turbo code will be low.

If recursive convolutional codes are used as constituent codes the probability is high, that at least one of the constituent codes generates a sequence with high Hamming weight.

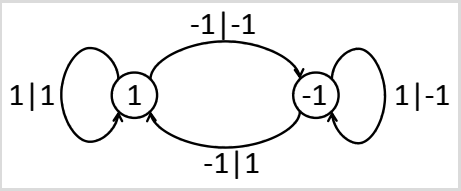
8.6 Differential Modulation with Viterbi Detector

A differential BPSK (D-BPSK) modulator as depicted in the following figure can be viewed as a recursive convolutional encoder with rate $R = 1$. Hint: $c_k \in \{\pm 1\}$.



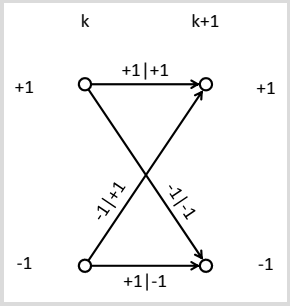
a) Determine the state transition diagram of the differential modulator.

Solution:



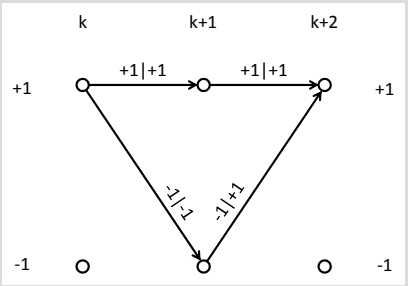
b) Determine the trellis butterfly of the differential modulator.

Solution:



c) Determine the free distance of the differential modulation scheme.

Solution:



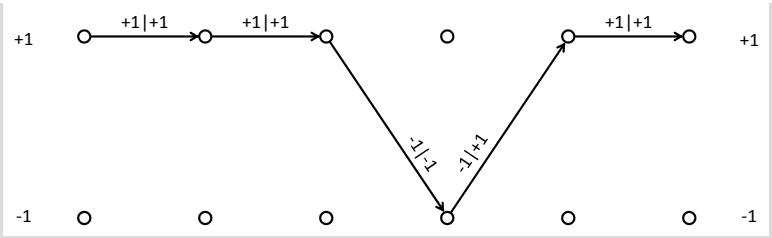
Determine the path that which diverges from the all +1 path and remerges with the all +1 path as soon as possible. The transmit sequence corresponding to this path is $\mathbf{d} = \begin{bmatrix} -1 & +1 \end{bmatrix}^T$. It differs from the all +1 sequence only in the first symbol. Therefore, the free distance is

$$d_f = 1.$$

This means that actually no errors can be corrected.

d) Sketch the trellis path for the transmit sequence $\mathbf{c} = \begin{bmatrix} +1 & +1 & -1 & -1 & +1 \end{bmatrix}^T$. Assume that the differential encoder is initialized in state +1 at the beginning of the sequence. Which sequence $\mathbf{d}$ is transmitted?

Solution:



$$\mathbf{d} = \begin{bmatrix} +1 \\ +1 \\ -1 \\ +1 \\ +1 \end{bmatrix}$$

e) Derive the metric increments of an APP and an ML Viterbi detector for differential modulation using log-likelihood ratios.

The metric increment $\Delta\mu_k(s_i, s_j)$ is used to calculate the metric $\mu_k(s_j)$ along a path of the trellis.

$$\mu_k(s_j) = \max_i \{\mu_{k-1}(s_i) + \Delta\mu_k(s_i, s_j)\}$$

To derive the metric increment, first consider the following:

$$\begin{aligned} L_c(d_k) &= \log \frac{P(y_k|d_k = 1)}{P(y_k|d_k = -1)} \\ \Rightarrow P(y_k|d_k = 1) &= \frac{e^{L_c(d_k)}}{1 + e^{L_c(d_k)}} = \frac{e^{\frac{L_c(d_k)}{2}}}{1 + e^{L_c(d_k)}} e^{d_k \frac{L_c(d_k)}{2}} \\ P(y_k|d_k = -1) &= \frac{1}{1 + e^{L_c(d_k)}} = \frac{e^{\frac{L_c(d_k)}{2}}}{1 + e^{L_c(d_k)}} e^{d_k \frac{L_c(d_k)}{2}} \end{aligned}$$

Thus, the probability $P(y_k|d_k)$ can be expressed as

$$P(y_k|d_k) = \text{const}_1 \cdot e^{d_k \frac{L_c(d_k)}{2}},$$

with $\text{const}_1 = \frac{e^{\frac{L_c(d_k)}{2}}}{1+e^{L_c(d_k)}}$.

Similarly, show that $P_a(c_k) = \text{const}_2 \cdot e^{c_k \frac{L_a(c_k)}{2}}$.

Therefore, $\log P(d_k|y_k)$ can be written as

$$\begin{aligned} \log P(d_k|y_k) &= \log \frac{P(y_k|d_k)P(d_k)}{P(y_k)} \\ &= \log\left(P(y_k|d_k)\right) + \log\left(P(c_k)\right) - \log\left(P(y_k)\right) \\ &= \log\left(\text{const}_1\right) + \log\left(e^{d_k \frac{L_c(d_k)}{2}}\right) + \log\left(\text{const}_2\right) + \log\left(e^{c_k \frac{L_a(c_k)}{2}}\right) - \log\left(P(y_k)\right) \\ &= \text{const}_3 + d_k \frac{L_c(d_k)}{2} + c_k \frac{L_a(c_k)}{2}, \end{aligned}$$

where $\text{const}_3 = \log\left(\text{const}_1\right) + \log\left(\text{const}_2\right) - \log\left(P(y_k)\right)$.

As constant terms are not relevant for the maximum, just consider the non constant terms.

Thus, the metric increment for APP decoding is given by

APP:

$$\Delta\mu_k(s_i, s_j) = d_k(s_i, s_j)\frac{L_c(d_k)}{2} + c_k(s_i, s_j)\frac{L_a(c_k)}{2}$$

ML: For ML decoding, the a priori information is not considered and therefore the metric increment is

$$\Delta\mu_k(s_i, s_j) = d_k(s_i, s_j)L_c(d_k)$$

Assume that the sequence $\mathbf{c}$ from d) has been transmitted through an AWGN channel with an SNR of 10 dB. The received sequence is given by

$$\mathbf{y} = \begin{bmatrix} +2.0 & -0.1 & -0.5 & +0.1 & +1.0 \end{bmatrix}^T$$

The source statistics are given by $P(c_k = +1) = \frac{1}{4}$, $P(c_k = -1) = \frac{3}{4}$.

f) Determine the estimated sequence using the Viterbi algorithm for the following cases:

For MAP decoding the a priori L-value is necessary. For all k it is given by

$$L_a(c_k) = \log\frac{P(c_k = 1)}{P(c_k = -1)} = \log\frac{\frac{1}{4}}{\frac{3}{4}} = \log\frac{1}{3} \approx -1.1.$$

For the channel L-values $L_c(d_k)$ we need the noise power:

$$\begin{aligned} 10\log_{10}\frac{\mathrm{P_X}}{\mathrm{P_N}}\ \mathrm{dB} &= 10\ \mathrm{dB} \\ \Leftrightarrow \frac{P_X}{P_N} = \frac{1}{\sigma_N^2} &= 10^{\frac{10}{10}} = 10 \\ \Leftrightarrow \sigma_N^2 &= 0.1 \end{aligned}$$

Then, we can calculate the channel L-value in the following way:

$$\begin{aligned} L_c(d_k) &= \log\frac{P(y_k|d_k = 1)}{P(y_k|d_k = -1)} \\ &= \log\frac{\frac{1}{\sqrt{2\pi}\sigma_N}e^{-\frac{(y_k-1)^2}{2\sigma_N^2}}}{\frac{1}{\sqrt{2\pi}\sigma_N}e^{-\frac{(y_k+1)^2}{2\sigma_N^2}}} \\ &= \log e^{-\frac{(y_k-1)^2}{2\sigma_N^2}+\frac{(y_k+1)^2}{2\sigma_N^2}} \\ &= -\frac{(y_k-1)^2}{2\sigma_N^2} + \frac{(y_k+1)^2}{2\sigma_N^2} \\ &= \frac{1}{2\sigma_N^2}\left[-y_k^2 - 1 + 2y_k + y_k^2 + 1 + 2y_k\right] \\ &= \frac{1}{0.2}4y_k \\ &= 20y_k \end{aligned}$$

The hard decision values of $\mathbf{y}$ are $\hat{\mathbf{y}} = \begin{bmatrix} +1 & -1 & -1 & +1 & +1 \end{bmatrix}^T$.

(1) Hard decision maximum likelihood (ML) sequence estimation.

Solution:

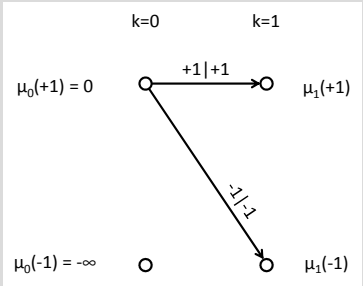
$$\Delta\mu_k(s_i, s_j) = d_k(s_i, s_j)L_c(d_k) = d_k(s_i, s_j)20y_k$$

The factor 20 is the same for all paths and therefore does not influence where the

metric achieves its maximum. Thus, it can be ignored and the metric increment reduces to $\Delta\mu_k(s_i, s_j) = d_k(s_i, s_j)y_k$. As here only the hard values are used, we end up with

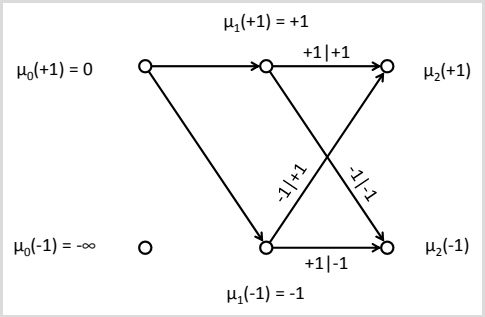
$$\Delta\mu_k(s_i, s_j) = d_k(s_i, s_j)\hat{y}_k\,.$$

First, start in state $s_i = +1$ at time step $k = 0$. Initialize the metric with $\mu_0(+1) = \log 1 = 0$ and $\mu_0(-1) = -\infty$.



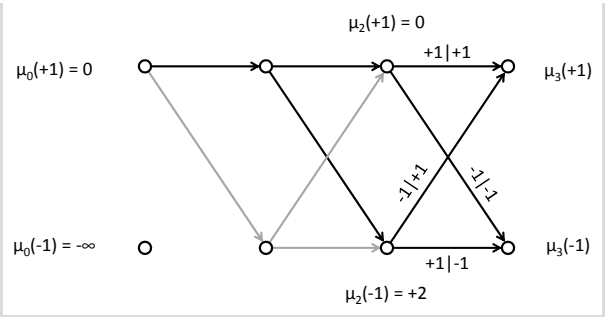
$$\begin{aligned}
\mu_1(+1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,+1), \mu_0(-1) + \Delta\mu_1(-1,+1)\} \\
&= \max\{0 + 1\cdot 1, -\infty + 1\cdot 1\} = \max\{1, -\infty\} = 1 \\
\mu_1(-1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,-1), \mu_0(-1) + \Delta\mu_1(-1,-1)\} \\
&= \max\{0 + 1\cdot(-1), -\infty + 1\cdot(-1)\} = \max\{-1, -\infty\} = -1
\end{aligned}$$

As the paths starting in $s_i = -1$ have a smaller metric than those stating in $s_i = +1$ they need not to be considered further.

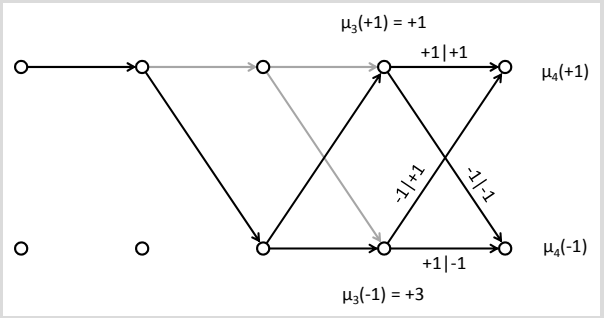


$$\begin{aligned}
\mu_2(+1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,+1), \mu_1(-1) + \Delta\mu_2(-1,+1)\} \\
&= \max\{1 + 1\cdot(-1), -1 + 1\cdot(-1)\} = \max\{0, -2\} = 0 \\
\mu_2(-1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,-1), \mu_1(-1) + \Delta\mu_2(-1,-1)\} \\
&= \max\{1 + (-1)\cdot(-1), -1 + (-1)\cdot(-1)\} = \max\{2, 0\} = 2
\end{aligned}$$

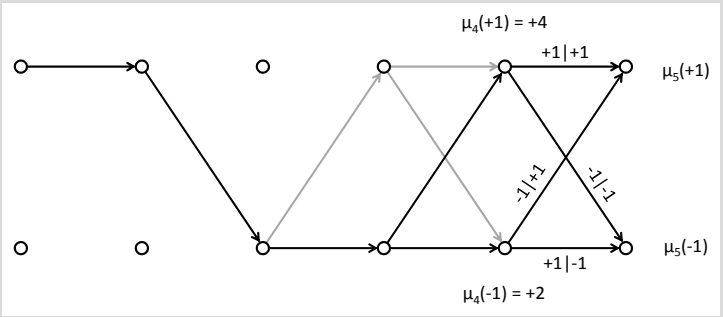
For all states, delete all paths ending in that state that do not have the maximal metric. This means, that the paths with metric 0 in state -1 are canceled, as the metric of the other paths in the same states are larger. Thus, the trellis reduces as shown in the next figure.



$$\begin{aligned}\mu_3(+1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,+1), \mu_2(-1) + \Delta\mu_3(-1,+1)\} \\ &= \max\{0 + 1\cdot(-1), 2 + 1\cdot(-1)\} = \max\{-1, 1\} = 1 \\ \mu_3(-1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,-1), \mu_2(-1) + \Delta\mu_3(-1,+1)\} \\ &= \max\{0 + (-1)\cdot(-1), 2 + (-1)\cdot(-1)\} = \max\{1, 3\} = 3\end{aligned}$$

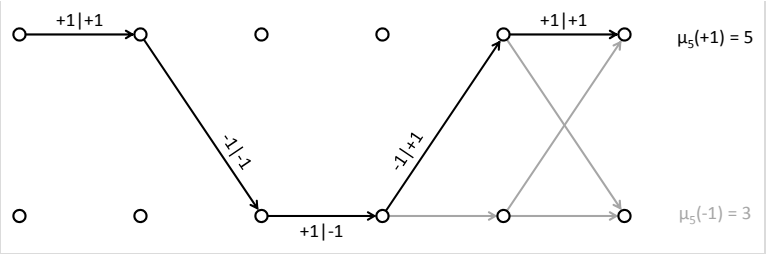


$$\begin{aligned}\mu_4(+1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,+1), \mu_3(-1) + \Delta\mu_4(-1,+1)\} \\ &= \max\{1 + 1\cdot 1, 3 + 1\cdot 1\} = \max\{2, 4\} = 4 \\ \mu_4(-1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,-1), \mu_3(-1) + \Delta\mu_4(-1,-1)\} \\ &= \max\{1 + (-1)\cdot 1, 3 + (-1)\cdot 1\} = \max\{0, 2\} = 2\end{aligned}$$



$$\begin{aligned}\mu_5(+1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,+1), \mu_4(-1) + \Delta\mu_5(-1,+1)\} \\ &= \max\{4 + 1\cdot 1, 2 + 1\cdot 1\} = \max\{5, 3\} = 5 \\ \mu_5(-1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,-1), \mu_4(-1) + \Delta\mu_5(-1,-1)\} \\ &= \max\{4 + (-1)\cdot 1, 2 + (-1)\cdot 1\} = \max\{3, 1\} = 3\end{aligned}$$

The path with the maximal metric is the one ending in state +1 at step 5 with metric 5. Thus, this is the most likely path trough the trellis considering ML detection. Thus, the ML path is:

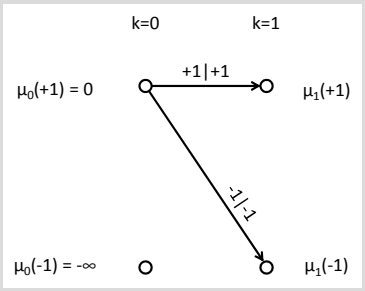


And, therefore, the detected sequence is $\hat{\mathbf{c}} = \begin{bmatrix} +1 & -1 & +1 & -1 & +1 \end{bmatrix}^T$.

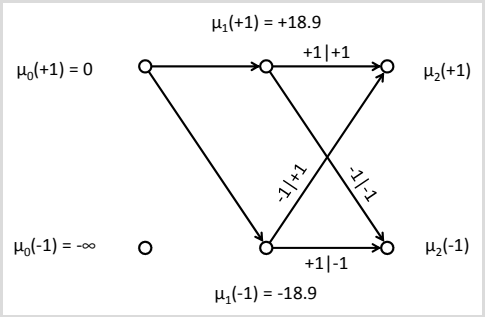
(2) Hard decision maximum a posteriori probability (MAP) sequence estimation.

For MAP detection the a priori information is also used. Therefore, the metric increment is given by

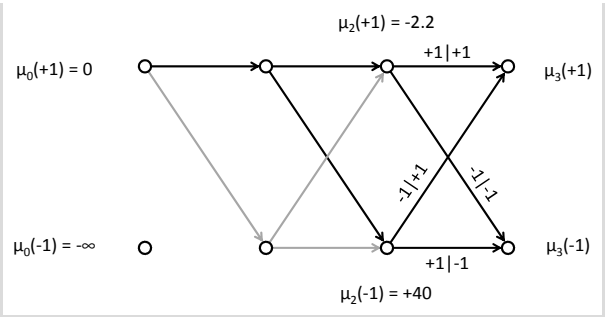
$$\Delta\mu_k = d_k(s_i, s_j)L_c(d_k) + c_k(s_i, s_j)L(c_k) = 20d_k(s_i, s_j)\hat{y_k} - 1.1c_k(s_i, s_j)$$



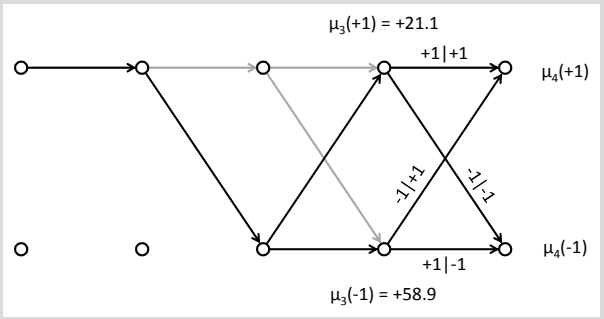
$$\begin{aligned}
\mu_1(+1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,+1), \mu_0(-1) + \Delta\mu_1(-1,+1)\} \\
&= \max\{0 + 20 \cdot 1 \cdot 1 - 1.1 \cdot 1, -\infty + 20 \cdot 1 \cdot 1 - 1.1 \cdot (-1)\} \\
&= \max\{18.9, -\infty\} = 18.9 \\
\mu_1(-1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,-1), \mu_0(-1) + \Delta\mu_1(-1,-1)\} \\
&= \max\{0 + 20 \cdot 1 \cdot (-1) - 1.1 \cdot (-1), -\infty + 20 \cdot 1 \cdot (-1) - 1.1 \cdot 1\} \\
&= \max\{-18.9, -\infty\} = -18.9
\end{aligned}$$



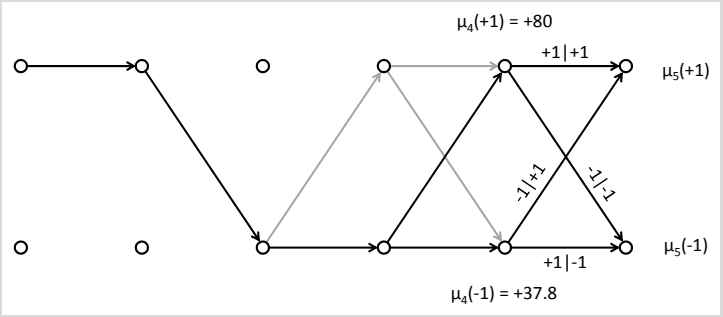
$$\begin{aligned}
\mu_2(+1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,+1), \mu_1(-1) + \Delta\mu_2(-1,+1)\} \\
&= \max\{18.9 + 20 \cdot 1 \cdot (-1) - 1.1 \cdot 1, -18.9 + 20 \cdot 1 \cdot (-1) - 1.1 \cdot (-1)\} \\
&= \max\{-2.2, -37.8\} = -2.2 \\
\mu_2(-1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,-1), \mu_1(S_2) + \Delta\mu_2(-1,-1)\} \\
&= \max\{-18.9 + 20 \cdot (-1) \cdot (-1) - 1.1 \cdot (-1), 18.9 + 20 \cdot (-1) \cdot (-1) - 1.1 \cdot 1\} \\
&= \max\{40, 0\} = 40
\end{aligned}$$



$$\begin{aligned}
\mu_3(+1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,+1), \mu_2(-1) + \Delta\mu_3(-1,+1)\} \\
&= \max\{-2.2 + 20 \cdot 1 \cdot (-1) - 1.1 \cdot 1, 40 + 20 \cdot 1 \cdot (-1) - 1.1 \cdot (-1)\} \\
&= \max\{-23.3, 21.1\} = 21.1 \\
\mu_3(-1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,-1), \mu_2(-1) + \Delta\mu_3(-1,-1)\} \\
&= \max\{-2.2 + 20 \cdot (-1) \cdot (-1) - 1.1 \cdot (-1), 40 + 20 \cdot (-1) \cdot (-1) - 1.1 \cdot 1\} \\
&= \max\{18.9, 58.9\} = 58.9
\end{aligned}$$

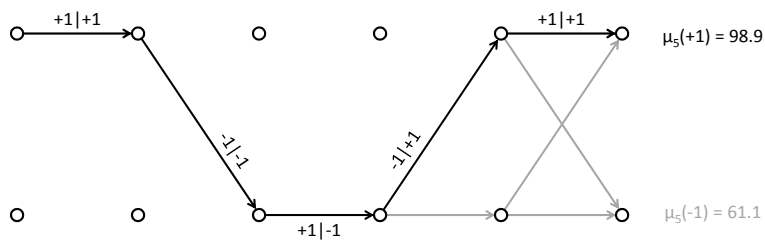


$$\begin{aligned}
\mu_4(+1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,+1), \mu_3(-1) + \Delta\mu_4(-1,+1)\} \\
&= \max\{21.1 + 20 \cdot 1 \cdot 1 - 1.1 \cdot 1, 58.9 + 20 \cdot 1 \cdot 1 - 1.1 \cdot (-1)\} \\
&= \max\{40, 80\} = 80 \\
\mu_4(-1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,-1), \mu_3(-1) + \Delta\mu_4(-1,-1)\} \\
&= \max\{21.1 + 20 \cdot (-1) \cdot 1 - 1.1 \cdot (-1), 58.9 + 20 \cdot (-1) \cdot 1 - 1.1 \cdot 1\} \\
&= \max\{2.2, 37.8\} = 37.8
\end{aligned}$$



$$
\begin{aligned}
\mu_5(+1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,+1), \mu_4(-1) + \Delta\mu_5(-1,+1)\} \\
&= \max\{80 + 20\cdot 1\cdot 1 - 1.1\cdot 1, 37.8 + 20\cdot 1\cdot 1 - 1.1\cdot(-1)\} \\
&= \max\{98.9, 58.9\} = 98.9 \\
\mu_5(-1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,-1), \mu_4(-1) + \Delta\mu_5(-1,-1)\} \\
&= \max\{80 + 20\cdot(-1)\cdot 1 - 1.1\cdot(-1), 37.8 + 20\cdot(-1)\cdot 1 - 1.1\cdot 1\} \\
&= \max\{6.11, 16.7\} = 61.1
\end{aligned}
$$

The path with the maximal metric is the one ending in state +1 at step 5 with metric 61.1. Thus, this is the most likely path trough the trellis considering MAP detection. Thus, the detected path is:

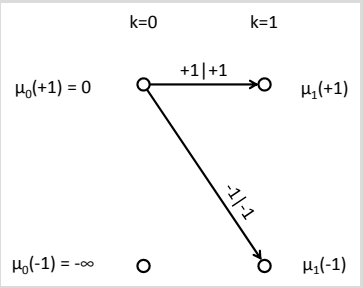


And, therefore, the detected sequence is $\hat{\mathbf{c}} = \begin{bmatrix} +1 & -1 & +1 & -1 & +1 \end{bmatrix}^T$.

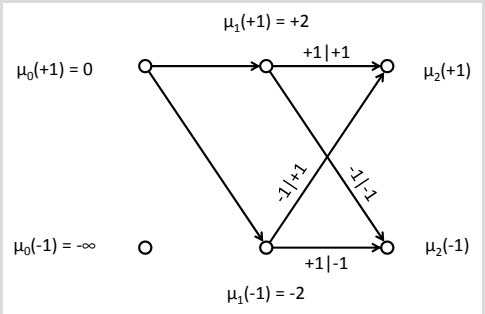
(3) Soft decision maximum likelihood (ML) sequence estimation.

In this case the metric increment is

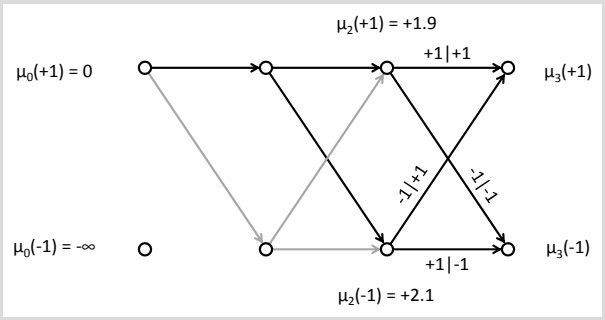
$$\Delta\mu_k = d_k(s_i, s_j) y_k$$



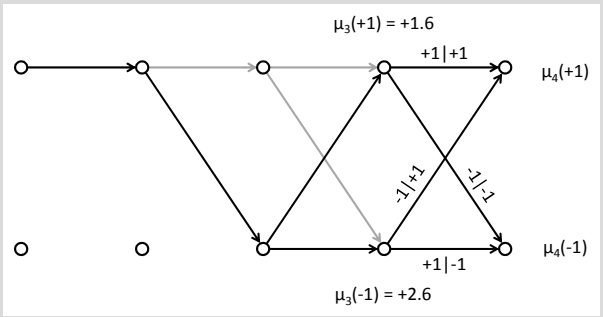
$$
\begin{aligned}
\mu_1(+1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,+1), \mu_0(-1) + \Delta\mu_1(-1,+1)\} \\
&= \max\{0 + 2\cdot 1, -\infty + 2\cdot 1\} = \max\{2, -\infty\} = 2 \\
\mu_1(-1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,-1), \mu_0(-1) + \Delta\mu_1(-1,-1)\} \\
&= \max\{0 + 2\cdot(-1), -\infty + 1\cdot(-1)\} = \max\{-2, -\infty\} = -2
\end{aligned}
$$



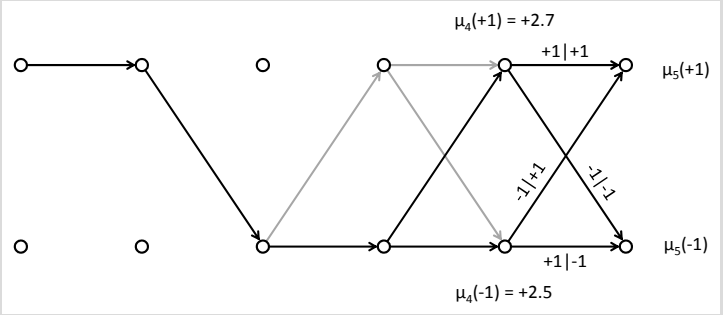
$$\begin{aligned}\mu_2(+1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,+1), \mu_1(-1) + \Delta\mu_2(-1,+1)\} \\ &= \max\{2 + 1\cdot(-0.1), -2 + 1\cdot(-0.1)\} = \max\{1.9, -2.1\} = 1.9 \\ \mu_2(-1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,-1), \mu_1(-1) + \Delta\mu_2(-1,-1)\} \\ &= \max\{2 + (-1)\cdot(-0.1), -2 + (-1)\cdot(-0.1)\} = \max\{2.1, -1.9\} = 2.1\end{aligned}$$



$$\begin{aligned}\mu_3(+1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,+1), \mu_2(-1) + \Delta\mu_3(-1,+1)\} \\ &= \max\{1.9 + 1\cdot(-0.5), 2.1 + 1\cdot(-0.5)\} = \max\{1.4, 1.6\} = 1.6 \\ \mu_3(-1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,-1), \mu_2(-1) + \Delta\mu_3(-1,-1)\} \\ &= \max\{1.9 + (-1)\cdot(-0.5), 2.1 + (-1)\cdot(-0.5)\} = \max\{2.4, 2.6\} = 2.6\end{aligned}$$

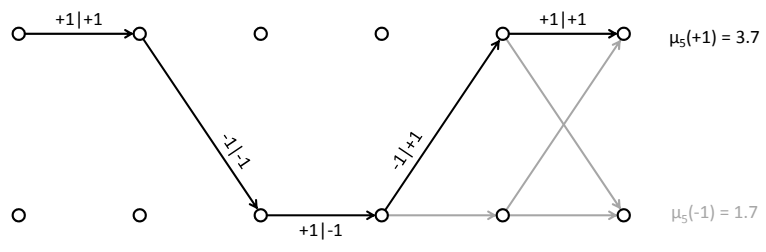


$$\begin{aligned}\mu_4(+1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,+1), \mu_3(-1) + \Delta\mu_4(-1,+1)\} \\ &= \max\{1.6 + 1\cdot 0.1, 2.6 + 1\cdot 0.1\} = \max\{1.7, 2.7\} = 2.7 \\ \mu_4(-1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,-1), \mu_3(-1) + \Delta\mu_4(-1,-1)\} \\ &= \max\{1.6 + (-1)\cdot 0.1, 2.6 + 20\cdot(-1)\cdot 0.1\} = \max\{1.5, 2.5\} = 2.5\end{aligned}$$



$$\begin{aligned}\mu_5(+1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,+1), \mu_4(-1) + \Delta\mu_5(-1,+1)\} \\ &= \max\{2.7 + 1\cdot 1, 2.5 + 1\cdot 1\} = \max\{3.7, 3.5\} = 3.7 \\ \mu_5(-1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,+1), \mu_4(-1) + \Delta\mu_5(-1,+1)\} \\ &= \max\{2.7 + (-1)\cdot 1, 2.5 + (-1)\cdot 1\} = \max\{1.7, 1.5\} = 1.7\end{aligned}$$

The path with the maximal metric is the one ending in state +1 at step 5 with metric 3.7. Thus, this is the most likely path trough the trellis considering ML detection. Thus, the detected path is:

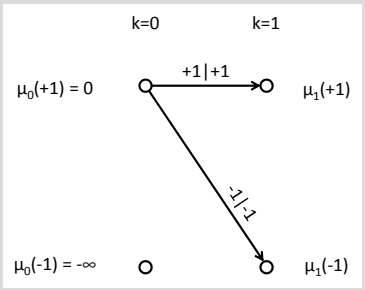


And, therefore, the detected sequence is $\hat{\mathbf{c}}_k = \begin{bmatrix}+1 & -1 & +1 & -1 & +1\end{bmatrix}^T$.

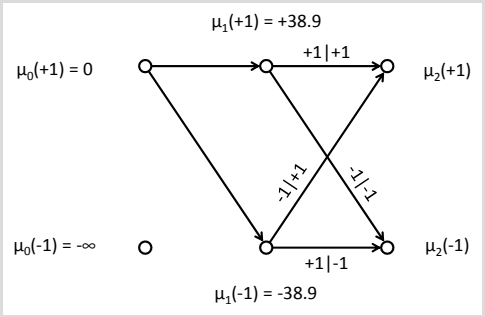
(4) Soft decision maximum a posteriori probability (MAP) sequence estimation.

In this case the metric increment is

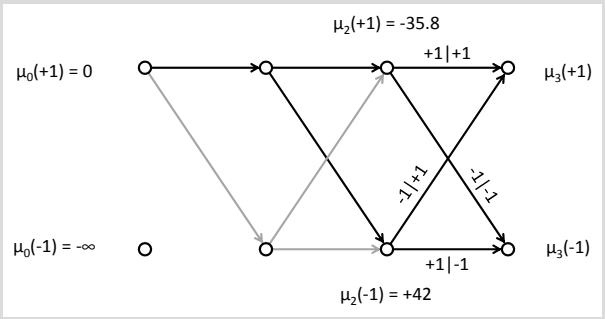
$$\Delta\mu_k = 20 d_k(s_i, s_j) y_k - 1.1 c_k(s_i, s_j)$$



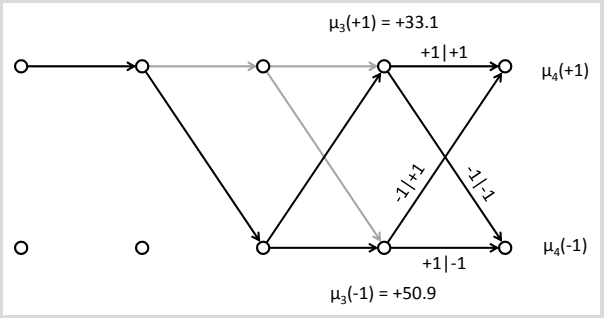
$$\begin{aligned}\mu_1(+1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,+1), \mu_0(-1) + \Delta\mu_1(-1,+1)\} \\ &= \max\{0 + 20\cdot 2\cdot 1 - 1.1\cdot 1, -\infty + 20\cdot 1\cdot 1 - 1.1\cdot(-1)\} \\ &= \max\{38.9, -\infty\} = 38.9 \\ \mu_1(-1) &= \max\{\mu_0(+1) + \Delta\mu_1(+1,-1), \mu_0(-1) + \Delta\mu_1(-1,-1)\} \\ &= \max\{0 + 20\cdot 2\cdot(-1) - 1.1\cdot(-1), -\infty + 20\cdot 2\cdot(-1) - 1.1\cdot 1\} \\ &= \max\{-38.9, -\infty\} = -38.9\end{aligned}$$



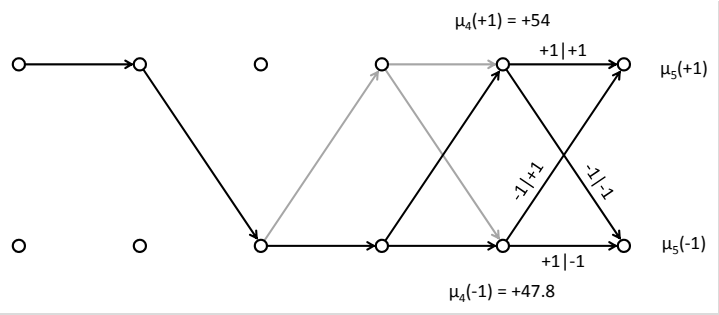
$$
\begin{aligned}
\mu_2(+1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,+1), \mu_1(-1) + \Delta\mu_2(-1,+1)\} \\
&= \max\{38.9 + 20 \cdot 1 \cdot (-0.1) - 1.1 \cdot 1, -38.9 + 20 \cdot 1 \cdot (-0.1) - 1.1 \cdot (-1)\} \\
&= \max\{-35.8, -39.8\} = 35.8 \\
\mu_2(-1) &= \max\{\mu_1(+1) + \Delta\mu_2(+1,-1), \mu_1(-1) + \Delta\mu_2(-1,-1)\} \\
&= \max\{38.9 + 20 \cdot (-1) \cdot (-0.1) - 1.1 \cdot (-1), -38.9 + 20 \cdot (-1) \cdot (-0.1) - 1.1 \cdot 1\} \\
&= \max\{42, -38\} = 42
\end{aligned}
$$



$$
\begin{aligned}
\mu_3(+1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,+1), \mu_2(-1) + \Delta\mu_3(-1,-1)\} \\
&= \max\{35.8 + 20 \cdot 1 \cdot (-0.5) - 1.1 \cdot 1, 42 + 20 \cdot 1 \cdot (-0.5) - 1.1 \cdot (-1)\} \\
&= \max\{24.7, 33.1\} = 33.1 \\
\mu_3(-1) &= \max\{\mu_2(+1) + \Delta\mu_3(+1,-1), \mu_2(-1) + \Delta\mu_3(-1,-1)\} \\
&= \max\{35.8 + 20 \cdot (-1) \cdot (-0.5) - 1.1 \cdot (-1), 42 + 20 \cdot (-1) \cdot (-0.5) - 1.1 \cdot 1\} \\
&= \max\{46.9, 50.9\} = 50.9
\end{aligned}
$$

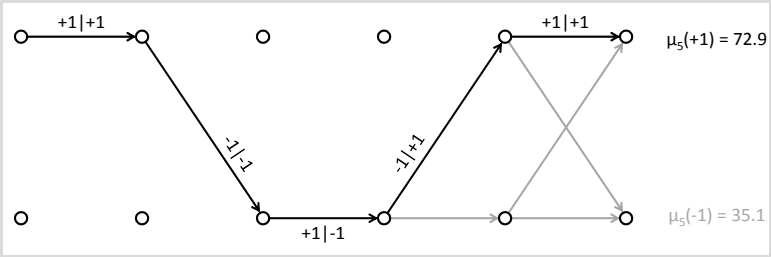


$$
\begin{aligned}
\mu_4(+1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,+1), \mu_3(-1) + \Delta\mu_4(-1,+1)\} \\
&= \max\{33.1 + 20 \cdot 1 \cdot 0.1 - 1.1 \cdot 1, 50.9 + 20 \cdot 1 \cdot 0.1 - 1.1 \cdot (-1)\} \\
&= \max\{34, 54\} = 54 \\
\mu_4(-1) &= \max\{\mu_3(+1) + \Delta\mu_4(+1,-1), \mu_3(-1) + \Delta\mu_4(-1,-1)\} \\
&= \max\{33.1 + 20 \cdot (-1) \cdot 0.1 - 1.1 \cdot (-1), 50.9 + 20 \cdot (-1) \cdot 0.1 - 1.1 \cdot 1\} \\
&= \max\{32.2, 47.8\} = 47.8
\end{aligned}
$$



$$
\begin{aligned}
\mu_5(+1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,+1), \mu_4(-1) + \Delta\mu_5(-1,+1)\} \\
&= \max\{54 + 20\cdot 1\cdot 1 - 1.1\cdot 1, 47.8 + 20\cdot 1\cdot 1 - 1.1\cdot(-1)\} \\
&= \max\{72.9, 68.9\} = 72.9 \\
\mu_5(-1) &= \max\{\mu_4(+1) + \Delta\mu_5(+1,-1), \mu_4(-1) + \Delta\mu_5(-1,-1)\} \\
&= \max\{54 + 20\cdot(-1)\cdot 1 - 1.1\cdot(-1), 47.8 + 20\cdot(-1)\cdot 1 - 1.1\cdot 1\} \\
&= \max\{35.1, 26.7\} = 35.1
\end{aligned}
$$

The path with the maximal metric is the one ending in state $+1$ at step 5 with metric 72.9. Thus, this is the most likely path trough the trellis considering MAP detection. Thus, the detected path is:



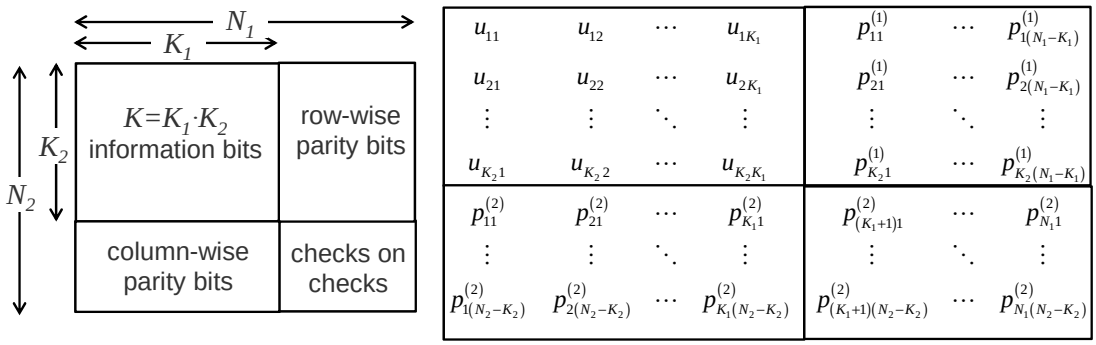
And, therefore, the detected sequence is $\hat{\mathbf{c}}_k = \begin{bmatrix} +1 & -1 & +1 & -1 & +1 \end{bmatrix}^T$.

Chapter 9

Special Block Codes

9.1 Product Code

The idea of a product code is to construct a powerful $(N,\ K)$ code by combining simple systematic linear $(N_i,\ K_i,\ d_{min,i})$ constituent block codes. The principle is depicted in the following figure:



The $K = K_1 \cdot K_2$ information bits are arranged in a $(K_1 \times K_2)$ matrix. Then, we encode first the rows using code 1. In a second step we encode the columns using code 2. The parity bits are appended as indicated in the figure. Furthermore, we encode the parity bits of code 1 column-wise using code 2 ("parity checks on parity checks").

a) What is the code rate R of the product code depending on the parameters N_i and K_i of the constituent codes?

Solution:

$$R = \frac{K}{N} = \frac{K_1 \cdot K_2}{N_1 \cdot N_2}$$

b) Determine the Singleton bound on the minimum Hamming distance d_{min} of the product code depending on the parameters N_i and K_i of the constituent codes.

Solution:

Singleton bound in general: $d_{min} \leq N - K + 1$

Singleton bound here: $d_{min} \leq N_1 N_2 - K_1 K_2 + 1$

c) Show, that the minimum Hamming distance d_{min} of the product code is given by the product $d_{min,1} \cdot d_{min,2}$ of the minimum Hamming distances of the constituent codes.

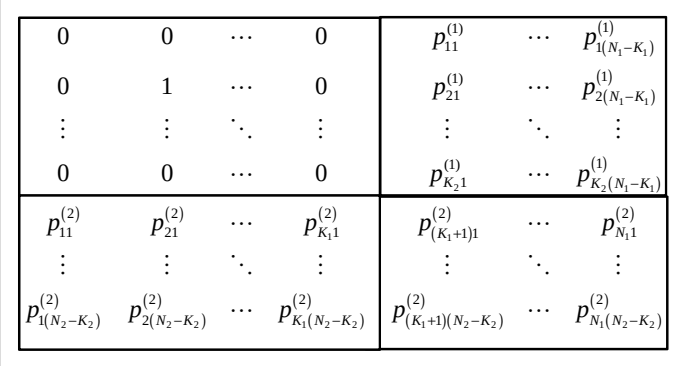
Solution:

In order to determine the minimum Hamming distance of a linear block code, it is sufficient to compare to the all-zeros codeword, i.e. it is sufficient to determine the

minimum Hamming weight w_{min}. We determine the minimum Hamming weight in two steps:

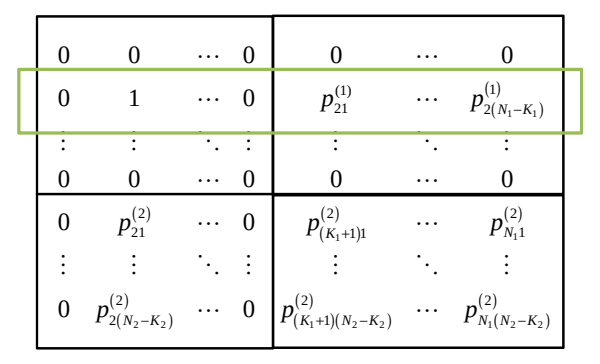
First, we show that the minimum weight (excluding the all-zeros codeword) is lower bounded by $w_{min} \leq d_{min,1} \cdot d_{min,2}$. In a second step, we show that codewords with this weight can be constructed.

Consider an information word which has just a single non-zero entry.

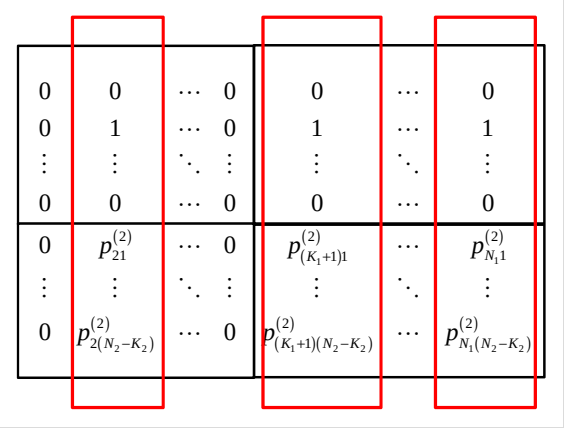


The parity bits for all columns and rows containing only zeros are also zero.

Consider the row which contains the 1:



As this row is a codeword of the code 1, it contains at least $d_{min,1}$ times a 1. Let w_r be the weight of this row. Then, $w_r \geq d_{min,1}$.



Now, consider all columns that contain a 1. All such columns will be equal to each other. As each column is a codeword of the code 2, it contains at least $d_{min,2}$ times a 1. Let w_c be weight of this column. Then, $w_c \geq d_{min,2}$. The weight w of this complete codeword is:

$$w = w_r \cdot w_c \geq d_{min,1} \cdot d_{min,2}$$

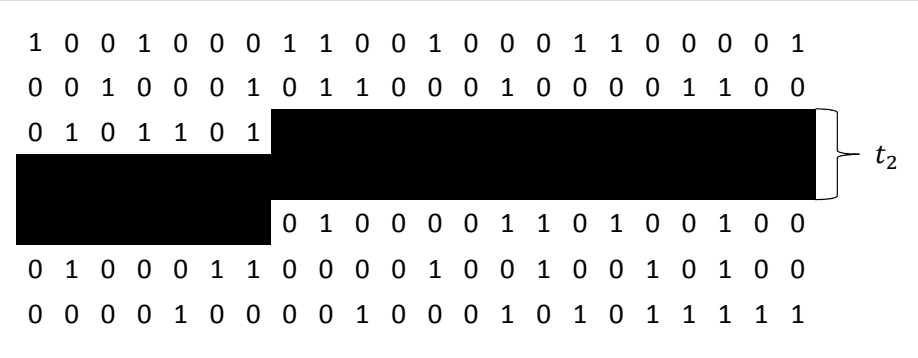
To construct such a codeword that has exactly weight $d_{min,1} \cdot d_{min,2}$, choose a codeword $\mathbf{x}_1$ from the code 1 with weight $d_{min,1}$. Choose a codeword $\mathbf{x}_2$ from the code 2 with weight $d_{min,2}$. If the i-th codebit of $\mathbf{x}_2$ is "1", place $\mathbf{x}_1$ in the i-th row of the product code matrix. Set all other rows to zero.

This type of code is called 'product code', because the minimal Hamming distance is given by the product of the minimal Hamming distances of the constituent codes.

d) Assume that the constituent code i can correct a burst error up to length t_i. What is the maximum length t of a burst error which can be corrected by the product code using a trivial decoding scheme which decodes successively column- and row-wise?

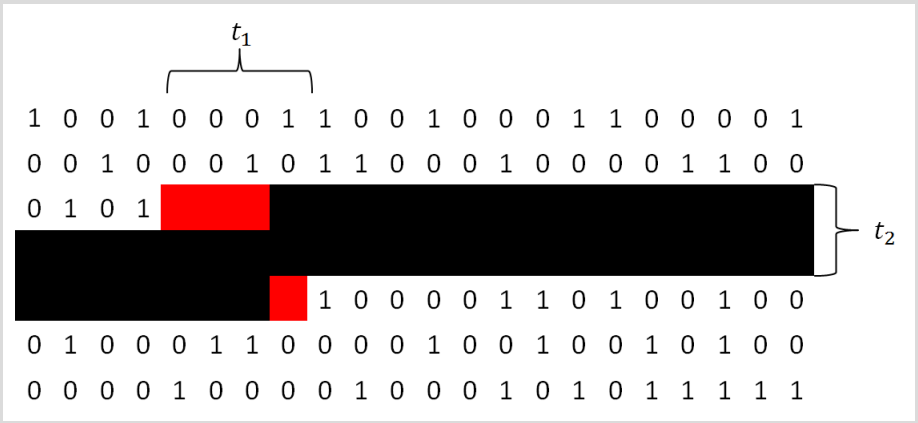
Solution:

Assume that the code bits are transmitted row-wise. Therefore, a burst error will affect a sequence of bits as indicated in the following figure.



As long as the burst error does not affect more than t_2 bits per column, the column-wise decoder will be able to decode all columns. Hence, a burst error up to length $N_1 \cdot t_2$ can be corrected by the column-wise decoder.

If the length of the error burst is $N_1 \cdot t_2 + t_1$ as depicted in the following figure t_1 columns will remain erroneous after column-wise decoding.



These erroneous columns can be corrected by the row-wise decoder. Therefore, an error burst up to length $N_1 \cdot t_2 + t_1$ can be corrected.

Alternatively, the code bits could be transmitted columns-wise. In this case, a burst error would affect a sequence of bits as indicated in the following figure.

When row-wise decoding is performed first, a burst error up to length $N_2 \cdot t_1 + t_2$ can be corrected.

If $N_1 \cdot t_2 + t_1 \geq N_2 \cdot t_1 + t_2$, the code bits should be transmitted row-wise and the decoder should first decode column-wise, than row-wise.

If $N_1 \cdot t_2 + t_1 \leq N_2 \cdot t_1 + t_2$, the code bits should be transmitted column-wise and the decoder should first decode row-wise, than column-wise.

With this strategy, the product code can correct burst errors up to length

$$\max(N_1 \cdot t_2 + t_1, N_2 \cdot t_1 + t_2)$$

e) Assume that the constituent code i can correct up to t_i single errors. How many single errors can at least be corrected by the product code?

Solution:

$$t_1 = \left\lfloor \frac{d_{min,1} - 1}{2} \right\rfloor \quad \Rightarrow \quad d_{min,1} \geq 2t_1 + 1$$
$$t_2 = \left\lfloor \frac{d_{min,2} - 1}{2} \right\rfloor \quad \Rightarrow \quad d_{min,2} \geq 2t_2 + 1$$

$$\begin{aligned} \Rightarrow t &= \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor \\ &= \left\lfloor \frac{d_{min,1} d_{min,2} - 1}{2} \right\rfloor \\ &\geq \left\lfloor \frac{(2t_1 + 1)(2t_2 + 1) - 1}{2} \right\rfloor \\ &= \left\lfloor \frac{4t_1 t_2 + 2t_1 + 2t_2 + 1 - 1}{2} \right\rfloor \\ &= 2t_1 t_2 + t_1 + t_2 \end{aligned}$$

We now assume that both constituent codes are $(7,\ 4,\ 3)_2$ Hamming codes.

f) Determine the parameters $(N,\ K,\ d_{min})_q$ of the product code.

Solution:

$$
\begin{aligned}
N &= N_1 N_2 = 7 \cdot 7 = 49 \\
K &= K_1 K_2 = 4 \cdot 4 = 16 \\
d_{min} &= d_{min,1} d_{min,2} = 3 \cdot 3 = 9 \\
q &= 2 \quad \text{(still binary)}
\end{aligned}
$$

The product code is a $(N_1 \cdot N_2, K_1 \cdot K_2, d_{\min,1} \cdot d_{\min,2})_q = (49,\ 16,\ 9)_2$ code.

g) How many errors should this product code correct according to the result of e)?

Solution:

For the $(7,\ 4,\ 3)_2$ code $t_i = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$. From e):

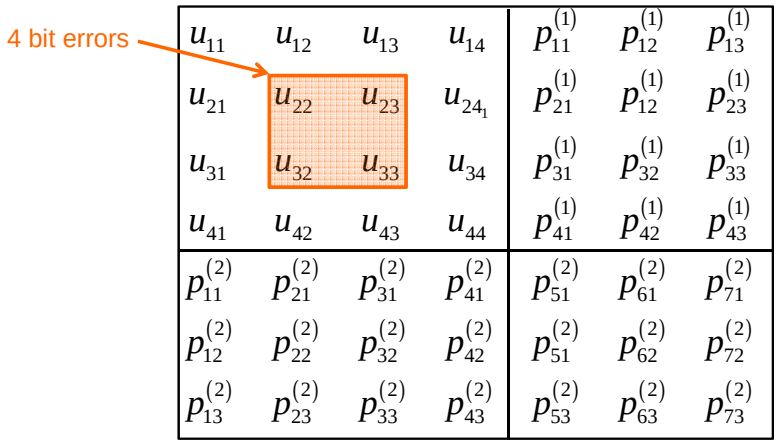
$$
\begin{aligned}
t &= 2 \cdot t_1 \cdot t_2 + t_1 + t_2 \\
&= 2 \cdot 1 \cdot 1 + 1 + 1 \\
&= 2 + 1 + 1 = 4\,.
\end{aligned}
$$

Alternative:

$$
t = \left\lfloor \frac{9-1}{2} \right\rfloor = 4
$$

h) Assume that four bit errors have occurred which are located in a square as indicated in the following figure. Is an error correction possible using a trivial decoding scheme which decodes successively column- and row-wise?

Solution:



The column-wise decoder can only correct a single error. Since the second and third column contain two errors each, both columns will be decoded wrong.

The row-wise decoder also can correct only a single error. Therefore, if the remaining errors of the column-wise decoder appear in the same rows, the row-wise decoder will also produce decoding errors.

$\Rightarrow$ A trivial decoding scheme which decodes all rows and columns separately can, in general, not correct this error pattern.
$\Rightarrow$ The potential of the product code is not exploited.
$\Rightarrow$ A more complex overall decoding scheme has to be applied in order to be able to correct all error patterns with up to four errors.

We now assume that both constituent codes are $(3,\ 2)_2$ single parity check codes.

i) Determine the parameters $(N,\ K,\ d_{min})_q$ of the product code.

Solution:

$$d_{min,1} = d_{min,2} = 2 \Rightarrow t_1 = t_2 = 0$$

$$\begin{aligned} N &= N_1 N_2 = 3 \cdot 3 = 9 \\ K &= K_1 K_2 = 2 \cdot 2 = 4 \\ d_{min} &= d_{min,1} d_{min,2} = 2 \cdot 2 = 4 \\ q &= 2 \quad \text{(still binary)} \end{aligned}$$

The product code is a $(9,\ 4,\ 4)_2$ code.

j) Determine the codeword for the info sequence $\mathbf{u} = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}^T$.

Solution:

The information is written as a (2×2) matrix:

0	1
1	1

Then, add the parity bits of the single parity check code row-wise

0	1	1
1	1	0

and column-wise

0	1	1
1	1	0
1	0	1

.

Transmit the codeword row-wise:

$$\mathbf{x} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T$$

k) How many errors can be corrected by a trivial decoding scheme which decodes successively column- and row-wise. Explain, how the errors can be localized.

Solution:

$t = 1$ error can be corrected using the trivial decoding scheme.

Suppose one error occurred. There is one row, where the check sum fails and one column where the check sum fails. The intersection of this row and column contains the error.

0	1	1	$\Rightarrow$ 0 $\oplus$ 1 $\oplus$ 1 =0 $\Rightarrow$ no error
1	0	0	$\Rightarrow$ 1 $\oplus$ 0 $\oplus$ 1 =1 $\Rightarrow$ error
1	0	1	$\Rightarrow$ 1 $\oplus$ 0 $\oplus$ 1 =0 $\Rightarrow$ no error
$\Downarrow$	$\Downarrow$	$\Downarrow$	
0$\oplus$1$\oplus$1 =0	1$\oplus$0$\oplus$0 =1	1$\oplus$0$\oplus$1 =0	
$\Downarrow$	$\Downarrow$	$\Downarrow$	
no error	error	no error	

l) How many candidate codewords have to be taken into consideration by a maximum likelihood (ML) decoder for the overall product code?

Solution:

The ML decoder has to compute $P(\mathbf{y}|\mathbf{x})$ for all $2^K = 2^{K_1 K_2} = 2^4 = 16$ possible codewords.

The decoded information word is obtained by $\hat{\mathbf{u}} = \arg\max_{\mathbf{u}\to\mathbf{x}} p(\mathbf{y}|\mathbf{x})$.

The number of candidate codewords grows exponentially with the block length K. Hence, also the complexity of the ML decoder grows exponentially with the block length K.

$\Rightarrow$ A suboptimal reduced complexity decoding scheme has to be found.

9.2 Sum Construction of Linear Block Codes

A powerful linear block code $\mathcal{C}$ is to be constructed of two simple linear block codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with the same codeword length $N_1 = N_2 = N$. $\mathcal{C}_1$ is a $(N,\ K_1,\ d_{min,1})_2$ code with generator matrix $\mathbf{G}_1$, $\mathcal{C}_2$ is a $(N,\ K_2,\ d_{min,2})_2$ code with generator matrix $\mathbf{G}_2$.
We define the following vectors:

Codeword of code $\mathcal{C}_i$: $\mathbf{x}_i = \begin{bmatrix} x_{i,1} \\ \vdots \\ x_{i,N} \end{bmatrix}$, $i = 1,\ 2$.

Information word of code $\mathcal{C}_i$: $\mathbf{u}_i = \begin{bmatrix} u_{i,1} \\ \vdots \\ u_{i,K_i} \end{bmatrix}$, $i = 1,\ 2$.

First we consider the following construction of code $\mathcal{C}$:

$$\mathcal{C} = \left\{ \mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \middle| \mathbf{x}_1 \in \mathcal{C}_1, \mathbf{x}_2 \in \mathcal{C}_2 \right\}$$

a) State the codeword length N', the information word length K and the code rate R of code $\mathcal{C}$.

Solution:

$$N' = N_1 + N_2 = 2N$$
$$K = K_1 + K_2$$
$$R = \frac{K_1 + K_2}{2N}$$

b) Determine the generator matrix $\mathbf{G}$ of code $\mathcal{C}$ dependent on the generator matrices $\mathbf{G}_1$ and $\mathbf{G}_2$.

Solution:

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1\mathbf{u}_1 \\ \mathbf{G}_2\mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{bmatrix} \begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{bmatrix} \mathbf{u}$$

$$\Rightarrow \mathbf{G} = \begin{bmatrix} \mathbf{G}_1 & 0 \\ 0 & \mathbf{G}_2 \end{bmatrix}$$

c) Determine the minimum Hamming distance d_{min} of code $\mathcal{C}$ dependent on $d_{min,1}$ and $d_{min,2}$.

Solution:

$$d_{min} = \min\{w_H(\mathbf{x}) | \mathbf{x} \in \mathcal{C}\} = \min(d_{min,1}, d_{min,2})$$

d) Determine the minimum Hamming distance d_{min} of code $\mathcal{C}$ dependent on $d_{min,1}$ and $d_{min,2}$ for the special case, that the code C_2 is a repetition code of rate $R_2 = \frac{1}{N}$.

Solution:

$\mathcal{C}_2$ repetition code $\Rightarrow d_{min,2} = N$ and $d_{min,1} \leq N$.

$$\Rightarrow d_{min} = \min(d_{min,1}, N) = d_{min,1}$$

From now on we consider the following construction of the code $\mathcal{C}$:

$$\mathcal{C} = \left\{ \mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_1 \oplus \mathbf{x}_2 \end{bmatrix} \middle| \mathbf{x}_1 \in \mathcal{C}_1, \mathbf{x}_2 \in \mathcal{C}_2 \right\} \tag{9.1}$$

where $\oplus$ is the modulo-2 addition.

e) Determine the generator matrix $\mathbf{G}$ of code $\mathcal{C}$ dependent of the generator matrices $\mathbf{G}_1$ and $\mathbf{G}_2$.

Solution:

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1\mathbf{u}_1 \\ \mathbf{G}_1\mathbf{u}_1 \oplus \mathbf{G}_2\mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{G}_1 & \mathbf{G}_2 \end{bmatrix} \begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{G}_1 & \mathbf{G}_2 \end{bmatrix} \mathbf{u}$$

$$\Rightarrow \mathbf{G} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{G}_1 & \mathbf{G}_2 \end{bmatrix}$$

f) Determine the minimum Hamming distance of code $\mathcal{C}$ dependent on $d_{min,1}$ and $d_{min,2}$.

Help:

- First consider the special cases $\mathbf{x}_1 = \mathbf{0}$ and $\mathbf{x}_2 = \mathbf{0}$.
- Then consider all other cases using the triangle inequality: $w_H(\mathbf{x} \oplus \mathbf{y}) \leq w_H(\mathbf{x}) + w_H(\mathbf{y})$.

Solution:

$$\mathbf{x}_1 = \mathbf{0} \text{ und } w_H(\mathbf{x}_2) = d_{min,2} \Rightarrow \begin{bmatrix} 0 \\ \mathbf{x}_2 \end{bmatrix} \in \mathcal{C}; w_H\left(\begin{bmatrix} 0 \\ \mathbf{x}_2 \end{bmatrix}\right) = d_{min,2} \Rightarrow d_{min} \leq d_{min,2}$$

$$\mathbf{x}_2 = \mathbf{0} \text{ und } w_H(\mathbf{x}_1) = d_{min,1} \Rightarrow \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_1 \end{bmatrix} \in \mathcal{C}; w_H\left(\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_1 \end{bmatrix}\right) = 2 * d_{min,1} \Rightarrow d_{min} \leq 2d_{min,1}$$

$$\Rightarrow d_{min} \leq \min\left(2d_{min,1}, d_{min,2}\right)$$

For an arbitrary codeword

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_1 \oplus \mathbf{x}_2 \end{bmatrix} \in \mathcal{C}$$

with $\mathbf{x}_1, \mathbf{x}_2 \neq 0$ it holds:

$$\begin{aligned} w_H(\mathbf{x}) &= w_H\left(\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{0} \end{bmatrix}\right) + w_H\left(\begin{bmatrix} \mathbf{0} \\ \mathbf{x}_1 \oplus \mathbf{x}_2 \end{bmatrix}\right) \\ &= w_H\left(\mathbf{x}_1\right) + w_H\left(\mathbf{x}_1 \oplus \mathbf{x}_2\right) \\ &\geq w_H(\mathbf{x}_1 + \mathbf{x}_1 + \mathbf{x}_2) = w_H(\mathbf{x}_2) \geq d_{min,2}. \end{aligned}$$

$$\Rightarrow \text{ there is no codeword } \mathbf{x} \in \mathcal{C} \text{ with } w_H(\mathbf{x}) < \min(2d_{min,1}, d_{min,2})$$

$$\Rightarrow d_{min} = \min(2d_{min,1}, d_{min,2})$$

g) Determine the minimum Hamming distance d_{min} of code $\mathcal{C}$ dependent on $d_{min,1}$ and $d_{min,2}$ for the special case, that the code C_2 is a repetition code with rate $R_2 = \frac{1}{N}$.

Solution:

$$\Rightarrow d_{min} = \min(2d_{min,1}, N)$$

h) Compare the results of part g) with the results of part d). Which code construction generates the more powerful code? Explain your answer!

Solution:

g) $d_{min} = \min(2d_{min,1}, N)$

d) $d_{min} = d_{min,1}$

If $d_{min,1} = N$ then the minimum distance d_{min} is the same in both cases and both codes are equally powerful. If $d_{min,1} < N$, then it holds, that $d_{min,1} < \min(2d_{min,1}, N)$. Thus the minimum distance of part d) is smaller as the one in part g). Thus the code of part g) is stronger.

9.3 Random Codes

When Shannon published his famous paper in 1948, channel codes did not exist. Shannon's theorems have been proven based on the idea of random codes. In this problem, we will address binary random codes, which map information words of length K bits to codeword of length N bits. A random code is constructed by randomly choosing the codewords among all possible binary sequences of length N.

a) Construct a random code of rate $R = \frac{1}{2}$ with codeword length $N = 6$. State all the codewords and the mapping of information words to codewords in a table.

Solution:

Given $N = 6$ and $R = \frac{1}{2}$ we know that

$$K = R \cdot N = 3$$

Thus we need to assign randomly selected 6 bit sequences for each of $2^3 = 8$ possible 3-bit information bits sequences. This assignment should be unique. One possible random code is given as:

label	information word	codeword
c_0	000	010100
c_1	001	111011
c_2	010	001000
c_3	011	111101
c_4	100	110000
c_5	101	011010
c_6	110	100101
c_7	111	001111

b) How many different binary sequences of length N exist?

Solution:

There exist 2^N different binary N-bit sequences.

c) How many different binary sequences of length N with Hamming weight w exist?

Solution:

In a binary sequence of Hamming weight w, exactly w out of N bits are ones. Hence, the number of such sequences is $\binom{N}{w}$.

d) How many codewords exist for a binary $(N, K)_2$ code ?

Solution:

The number of valid, unique codewords is limited to 2^K.

e) Assume, that a random code has been constructed. We then randomly choose a binary sequence of length N. Determine the probability, that this randomly chosen sequence is a codeword.

Solution:

Only 2^K out of the 2^N possible sequences are the codewords. Therefore, for a randomly chosen sequence $\mathbf{x}$

$$P(\mathbf{x} \text{ is a codeword}) = \frac{2^K}{2^N} = 2^{K-N}.$$

f) Determine the expected number $E\{A_w\}$ of codewords with Hamming weight w for a random $(N, K)_2$ code.

Solution:

From task c) we know that the number of sequences with Hamming weight w is $\binom{N}{w}$. From task e) we know that the probability of a sequence being a codeword is 2^{K-N}. Therefore, the expected number of weight w codewords is

$$E\{A_w\} = 2^{K-N}\binom{N}{w}.$$

g) Is a random code in general a linear code ? Give reasons!

Solution:

For a code to be linear, the sum of any two valid codewords is also a valid codeword. This property cannot be guaranteed if a code is generated randomly. Therefore, a random code is not linear in general.

h) Which minimum Hamming distance $d_{\min}$ can be guaranteed by the random code construction?

Solution:

For any code, the codewords need to be unique. Thus, any two codewords of a code differ at least in one bit position. Therefore, only a minimum Hamming distance of 1 is guaranteed for randomly generated codes

i) Determine the minimum Hamming weight $w_{\min}$ of your code from a).

Solution:

Minimum Hamming weight of the code is 1, as shown in following table

label	information word	codeword	w_H
c_0	000	010100	2
c_1	001	111011	5
c_2	010	001000	1
c_3	011	111101	5
c_4	100	110000	2
c_5	101	011010	3
c_6	110	100101	3
c_7	111	001111	4

j) Determine the minimum Hamming distance $d_{\min}$ of your code from a).

Solution:

Comparison of all possible codeword pairs show that the minimum Hamming distance of the code is

$$d_H(c_0, c_4) = 2.$$