1

Introduction

The reliable transmission of information over noisy channels is one of the basic requirements of digital information and communication systems. Here, transmission is understood both as transmission in space, e.g. over mobile radio channels, and as transmission in time by storing information in appropriate storage media. Because of this requirement, modern communication systems rely heavily on powerful channel coding methodologies. For practical applications these coding schemes do not only need to have good coding characteristics with respect to the capability of detecting or correcting errors introduced on the channel. They also have to be efficiently implementable, e.g. in digital hardware within integrated circuits. Practical applications of channel codes include space and satellite communications, data transmission, digital audio and video broadcasting and mobile communications, as well as storage systems such as computer memories or the compact disc (Costello *et al.*, 1998).

In this introductory chapter we will give a brief introduction into the field of channel coding. To this end, we will describe the information theory fundamentals of channel coding. Simple channel models will be presented that will be used throughout the text. Furthermore, we will present the binary triple repetition code as an illustrative example of a simple channel code.

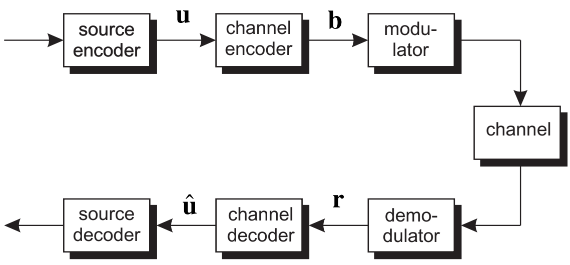
1.1 Communication Systems

In Figure 1.1 the basic structure of a digital communication system is shown which represents the architecture of the communication systems in use today. Within the transmitter of such a communication system the following tasks are carried out:

- source encoding,
- channel encoding,
- modulation.

Coding Theory – Algorithms, Architectures, and Applications André Neubauer, Jürgen Freudenberger, Volker Kühn

Principal structure of digital communication systems



- The sequence of information symbols **u** is encoded into the sequence of code symbols **b** which are transmitted across the channel after modulation.
- The sequence of received symbols **r** is decoded into the sequence of information symbols **û** which are estimates of the originally transmitted information symbols.

Figure 1.1: Basic structure of digital communication systems

In the receiver the corresponding inverse operations are implemented:

- demodulation,
- channel decoding,
- source decoding.

According to Figure 1.1 the *modulator* generates the signal that is used to transmit the sequence of symbols **b** across the channel (Benedetto and Biglieri, 1999; Neubauer, 2007; Proakis, 2001). Due to the noisy nature of the channel, the transmitted signal is disturbed. The noisy received signal is demodulated by the *demodulator* in the receiver, leading to the sequence of received symbols **r**. Since the received symbol sequence **r** usually differs from the transmitted symbol sequence **b**, a *channel code* is used such that the receiver is able to detect or even correct errors (Bossert, 1999; Lin and Costello, 2004; Neubauer, 2006b). To this end, the channel encoder introduces redundancy into the information sequence **u**. This redundancy can be exploited by the channel decoder for error detection or error correction by estimating the transmitted symbol sequence **û**.

In his fundamental work, Shannon showed that it is theoretically possible to realise an information transmission system with as small an error probability as required (Shannon, 1948). The prerequisite for this is that the information rate of the information source be smaller than the so-called channel capacity. In order to reduce the information rate, *source coding* schemes are used which are implemented by the source encoder in the transmitter and the source decoder in the receiver (McEliece, 2002; Neubauer, 2006a).

Further information about source coding can be found elsewhere (Gibson *et al*., 1998; Sayood, 2000, 2003).

In order better to understand the theoretical basics of information transmission as well as channel coding, we now give a brief overview of information theory as introduced by Shannon in his seminal paper (Shannon, 1948). In this context we will also introduce the simple channel models that will be used throughout the text.

1.2 Information Theory

An important result of information theory is the finding that error-free transmission across a noisy channel is theoretically possible – as long as the information rate does not exceed the so-called channel capacity. In order to quantify this result, we need to measure information. Within Shannon's information theory this is done by considering the statistics of symbols emitted by information sources.

1.2.1 Entropy

Let us consider the discrete memoryless *information source* shown in Figure 1.2. At a given time instant, this discrete information source emits the random discrete symbol $\mathcal{X} = x_i$ which assumes one out of M possible symbol values $x_1, x_2, \ldots, x_M$. The rate at which these symbol values appear are given by the probabilities $P_{\mathcal{X}}(x_1)$, $P_{\mathcal{X}}(x_2)$, …, $P_{\mathcal{X}}(x_M)$ with

$$P_{\mathcal{X}}(x_i) = \Pr\{\mathcal{X} = x_i\}.$$

Discrete information source

- The discrete information source emits the random discrete symbol $\mathcal{X}$.
- The symbol values $x_1, x_2, \ldots, x_M$ appear with probabilities $P_{\mathcal{X}}(x_1)$, $P_{\mathcal{X}}(x_2)$, …, $P_{\mathcal{X}}(x_M)$.
- Entropy

$$I(\mathcal{X}) = -\sum_{i=1}^{M} P_{\mathcal{X}}(x_i) \cdot \log_2(P_{\mathcal{X}}(x_i)) \qquad (1.1)$$

Figure 1.2: Discrete information source emitting discrete symbols $\mathcal{X}$

The average information associated with the random discrete symbol $\mathcal{X}$ is given by the so-called *entropy* measured in the unit 'bit'

$$I(\mathcal{X}) = -\sum_{i=1}^{M} P_{\mathcal{X}}(x_i) \cdot \log_2 \left(P_{\mathcal{X}}(x_i)\right).$$

For a binary information source that emits the binary symbols $\mathcal{X} = 0$ and $\mathcal{X} = 1$ with probabilities $\Pr\{\mathcal{X} = 0\} = p_0$ and $\Pr\{\mathcal{X} = 1\} = 1 - \Pr\{\mathcal{X} = 0\} = 1 - p_0$, the entropy is given by the so-called *Shannon function* or binary entropy function

$$I(\mathcal{X}) = -p_0 \log_2(p_0) - (1 - p_0) \log_2(1 - p_0).$$

1.2.2 Channel Capacity

With the help of the entropy concept we can model a channel according to Berger's channel diagram shown in Figure 1.3 (Neubauer, 2006a). Here, $\mathcal{X}$ refers to the input symbol and $\mathcal{R}$ denotes the output symbol or received symbol. We now assume that M input symbol values $x_1, x_2, \ldots, x_M$ and N output symbol values $r_1, r_2, \ldots, r_N$ are possible. With the help of the conditional probabilities

$$P_{\mathcal{X}|\mathcal{R}}(x_i|r_j) = \Pr\{\mathcal{X} = x_i|\mathcal{R} = r_j\}$$

and

$$P_{\mathcal{R}|\mathcal{X}}(r_j|x_i) = \Pr\{\mathcal{R} = r_j|\mathcal{X} = x_i\}$$

the conditional entropies are given by

$$I(\mathcal{X}|\mathcal{R}) = -\sum_{i=1}^{M}\sum_{j=1}^{N} P_{\mathcal{X},\mathcal{R}}(x_i, r_j) \cdot \log_2 \left(P_{\mathcal{X}|\mathcal{R}}(x_i|r_j)\right)$$

and

$$I(\mathcal{R}|\mathcal{X}) = -\sum_{i=1}^{M}\sum_{j=1}^{N} P_{\mathcal{X},\mathcal{R}}(x_i, r_j) \cdot \log_2(P_{\mathcal{R}|\mathcal{X}}(r_j|x_i)).$$

With these conditional probabilities the *mutual information*

$$I(\mathcal{X};\mathcal{R}) = I(\mathcal{X}) - I(\mathcal{X}|\mathcal{R}) = I(\mathcal{R}) - I(\mathcal{R}|\mathcal{X})$$

can be derived which measures the amount of information that is transmitted across the channel from the input to the output for a given information source.

The so-called *channel capacity* C is obtained by maximising the mutual information $I(\mathcal{X};\mathcal{R})$ with respect to the statistical properties of the input $\mathcal{X}$, i.e. by appropriately choosing the probabilities $\{P_{\mathcal{X}}(x_i)\}_{1 \le i \le M}$. This leads to

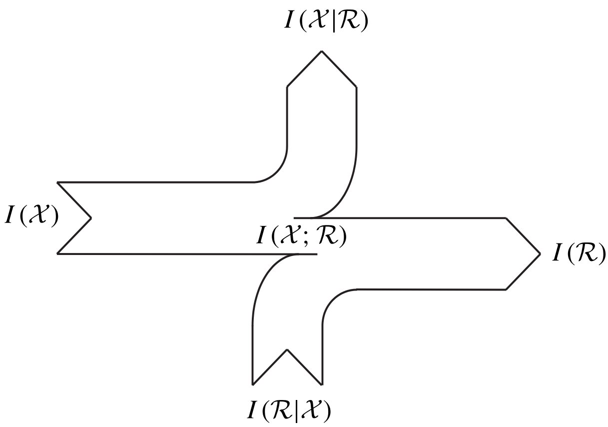
$$C = \max_{\{P_{\mathcal{X}}(x_i)\}_{1 \le i \le M}} I(\mathcal{X};\mathcal{R}).$$

If the input entropy $I(\mathcal{X})$ is smaller than the channel capacity C

$$I(\mathcal{X}) \overset{!}{<} C,$$

then information can be transmitted across the noisy channel with arbitrarily small error probability. Thus, the channel capacity C in fact quantifies the information transmission capacity of the channel.

Berger's channel diagram



- Mutual information

$$I(\mathcal{X};\mathcal{R}) = I(\mathcal{X}) - I(\mathcal{X}|\mathcal{R}) = I(\mathcal{R}) - I(\mathcal{R}|\mathcal{X}) \tag{1.2}$$

- Channel capacity

$$C = \max_{\{P_{\mathcal{X}}(x_i)\}_{1 \le i \le M}} I(\mathcal{X};\mathcal{R}) \tag{1.3}$$

Figure 1.3: Berger's channel diagram

1.2.3 Binary Symmetric Channel

As an important example of a memoryless channel we turn to the *binary symmetric channel* or BSC. Figure 1.4 shows the channel diagram of the binary symmetric channel with bit error probability ε. This channel transmits the binary symbol $\mathcal{X} = 0$ or $\mathcal{X} = 1$ correctly with probability $1 - \varepsilon$, whereas the incorrect binary symbol $\mathcal{R} = 1$ or $\mathcal{R} = 0$ is emitted with probability ε.

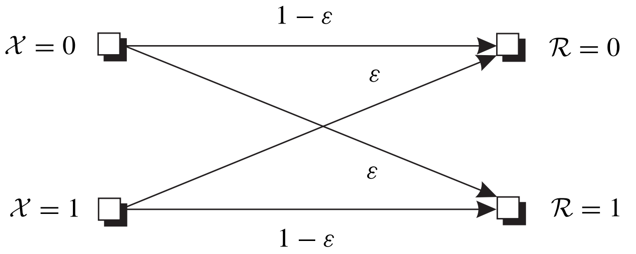
By maximising the mutual information $I(\mathcal{X};\mathcal{R})$, the channel capacity of a binary symmetric channel is obtained according to

$$C = 1 + \varepsilon \log_2(\varepsilon) + (1 - \varepsilon) \log_2(1 - \varepsilon).$$

This channel capacity is equal to 1 if $\varepsilon = 0$ or $\varepsilon = 1$; for $\varepsilon = \frac{1}{2}$ the channel capacity is 0. In contrast to the binary symmetric channel, which has discrete input and output symbols taken from binary alphabets, the so-called AWGN channel is defined on the basis of continuous real-valued random variables.[1]

[1]In Chapter 5 we will also consider complex-valued random variables.

Binary symmetric channel



- Bit error probability ε
- Channel capacity

$$C = 1 + \varepsilon \, \log_2(\varepsilon) + (1 - \varepsilon) \, \log_2(1 - \varepsilon) \tag{1.4}$$

Figure 1.4: Binary symmetric channel with bit error probability ε

1.2.4 AWGN Channel

Up to now we have exclusively considered discrete-valued symbols. The concept of entropy can be transferred to continuous real-valued random variables by introducing the so-called differential entropy. It turns out that a channel with real-valued input and output symbols can again be characterised with the help of the mutual information $I(\mathcal{X}; \mathcal{R})$ and its maximum, the channel capacity C. In Figure 1.5 the so-called *AWGN channel* is illustrated which is described by the additive white Gaussian noise term $\mathcal{Z}$.

With the help of the signal power

$$S = \mathrm{E}\left\{\mathcal{X}^2\right\}$$

and the noise power

$$N = \mathrm{E}\left\{\mathcal{Z}^2\right\}$$

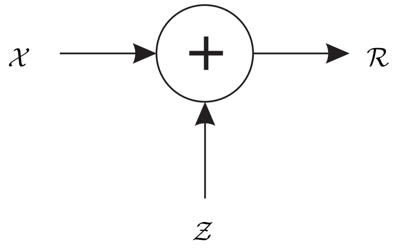
the channel capacity of the AWGN channel is given by

$$C = \frac{1}{2} \log_2 \left(1 + \frac{S}{N}\right).$$

The channel capacity exclusively depends on the signal-to-noise ratio S/N.

In order to compare the channel capacities of the binary symmetric channel and the AWGN channel, we assume a digital transmission scheme using binary phase shift keying (BPSK) and optimal reception with the help of a matched filter (Benedetto and Biglieri, 1999; Neubauer, 2007; Proakis, 2001). The signal-to-noise ratio of the real-valued output

AWGN channel



- Signal-to-noise ratio $\frac{S}{N}$
- Channel capacity

$$C = \frac{1}{2} \log_2 \left(1 + \frac{S}{N}\right) \tag{1.5}$$

Figure 1.5: AWGN channel with signal-to-noise ratio S/N

$\mathcal{R}$ of the matched filter is then given by

$$\frac{S}{N} = \frac{E_b}{N_0/2}$$

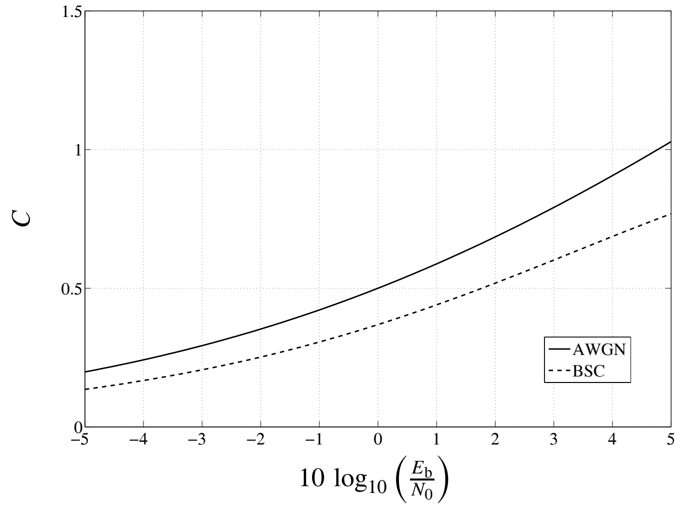
with bit energy E_b and noise power spectral density N_0. If the output $\mathcal{R}$ of the matched filter is compared with the threshold 0, we obtain the binary symmetric channel with bit error probability

$$\varepsilon = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right).$$

Here, erfc($\cdot$) denotes the complementary error function. In Figure 1.6 the channel capacities of the binary symmetric channel and the AWGN channel are compared as a function of E_b/N_0. The signal-to-noise ratio S/N or the ratio E_b/N_0 must be higher for the binary symmetric channel compared with the AWGN channel in order to achieve the same channel capacity. This gain also translates to the coding gain achievable by soft-decision decoding as opposed to hard-decision decoding of channel codes, as we will see later (e.g. in Section 2.2.8).

Although information theory tells us that it is theoretically possible to find a channel code that for a given channel leads to as small an error probability as required, the design of good channel codes is generally difficult. Therefore, in the next chapters several classes of channel codes will be described. Here, we start with a simple example.

Channel capacity of BSC vs AWGN channel



- Signal-to-noise ratio of AWGN channel

$$\frac{S}{N} = \frac{E_{\mathrm{b}}}{N_0/2} \tag{1.6}$$

- Bit error probability of binary symmetric channel

$$\varepsilon = \frac{1}{2}\,\mathrm{erfc}\left(\sqrt{\frac{E_{\mathrm{b}}}{N_0}}\right) \tag{1.7}$$

Figure 1.6: Channel capacity of the binary symmetric channel vs the channel capacity of the AWGN channel

1.3 A Simple Channel Code

As an introductory example of a simple channel code we consider the transmission of the binary information sequence

$$0\;0\;\underline{1}\;0\;\underline{1}\;1\;1\;0$$

over a binary symmetric channel with bit error probability $\varepsilon = 0.25$ (Neubauer, 2006b). On average, every fourth binary symbol will be received incorrectly. In this example we assume that the binary sequence

$$0\;0\;\underline{0}\;0\;\underline{0}\;1\;1\;0$$

is received at the output of the binary symmetric channel (see Figure 1.7).

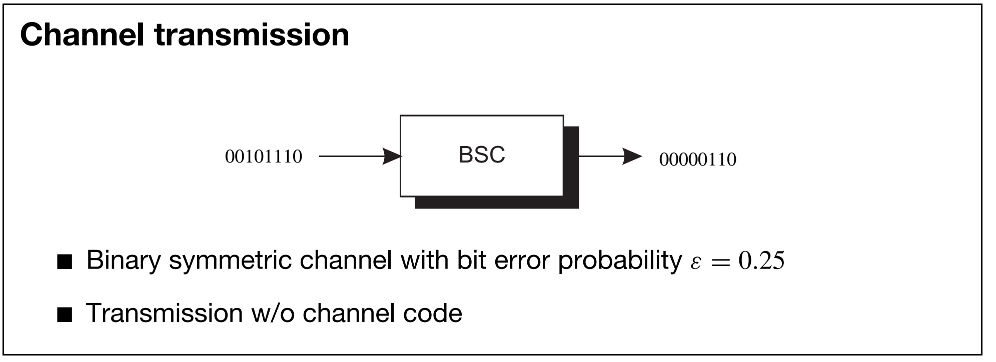


Figure 1.7: Channel transmission without channel code

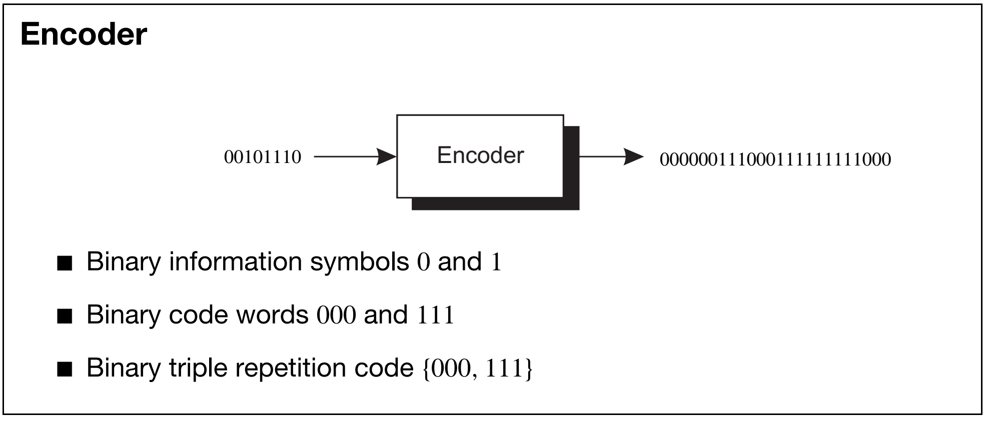


Figure 1.8: Encoder of a triple repetition code

In order to implement a simple error correction scheme we make use of the so-called binary *triple repetition code*. This simple channel code is used for the encoding of binary data. If the binary symbol 0 is to be transmitted, the encoder emits the code word 000. Alternatively, the code word 111 is issued by the encoder when the binary symbol 1 is to be transmitted. The encoder of a triple repetition code is illustrated in Figure 1.8.

For the binary information sequence given above we obtain the binary code sequence

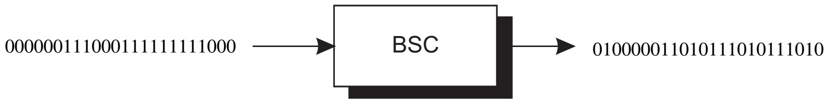
$$000\;000\;111\;000\;111\;111\;111\;000$$

at the output of the encoder. If we again assume that on average every fourth binary symbol is incorrectly transmitted by the binary symmetric channel, we may obtain the received sequence

$$0\underline{1}0\;000\;\underline{0}11\;0\underline{1}0\;111\;\underline{01}0\;111\;0\underline{1}0.$$

This is illustrated in Figure 1.9.

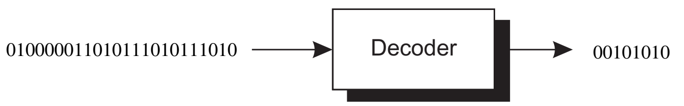
Channel transmission



- Binary symmetric channel with bit error probability $\varepsilon = 0.25$
- Transmission with binary triple repetition code

Figure 1.9: Channel transmission of a binary triple repetition code

Decoder



- Decoding of triple repetition code by majority decision

$$
\begin{aligned}
000 &\mapsto 000 \\
001 &\mapsto 000 \\
010 &\mapsto 000 \\
011 &\mapsto 111 \\
&\vdots \\
110 &\mapsto 111 \\
111 &\mapsto 111
\end{aligned}
$$

Figure 1.10: Decoder of a triple repetition code

The decoder in Figure 1.10 tries to estimate the original information sequence with the help of a *majority decision*. If the number of 0s within a received 3-bit word is larger than the number of 1s, the decoder emits the binary symbol 0; otherwise a 1 is decoded. With this decoding algorithm we obtain the decoded information sequence

$$0\,0\,1\,0\,1\,\underline{0}\,1\,0.$$

As can be seen from this example, the binary triple repetition code is able to correct a single error within a code word. More errors cannot be corrected. With the help of this simple channel code we are able to reduce the number of errors. Compared with the unprotected transmission without a channel code, the number of errors has been reduced from two to one. However, this is achieved by a significant reduction in the transmission bandwidth because, for a given symbol rate on the channel, it takes 3 times longer to transmit an information symbol with the help of the triple repetition code. It is one of the main topics of the following chapters to present more efficient coding schemes.