Block codes

Information transferred within an electronic communication channel is always liable to corruption by noise within the channel. Signals conveying information can be so contaminated by noise that the information becomes erroneous. It may be possible to reduce the level of noise but its complete elimination is not possible. The need therefore arises to be able to preserve the accuracy of information as it journeys through a noisy channel. Addressing this problem, Claude Shannon in 1948, showed that associated with every channel is an upper limit on the rate at which information can be transmitted reliably through the channel. This limitation on the capacity of a channel to transmit information is referred to as the *channel capacity*. Furthermore Shannon proved the existence of codes that enable information to be transmitted through a noisy channel such that the probability of errors is as small as required, providing that the transmission rate does not exceed the channel capacity. If information is transmitted at a rate greater than the channel capacity then it is not possible to achieve error-free transmission. Shannon's theoretical work on channel capacity and error-free transmission is now referred to as the *channel coding theorem*. The theorem does not say what the codes are or even how we go about finding them, it just proves their existence. It is a quite remarkable theorem as it tells us that there is no limit to the level of accuracy that can be achieved. It seems reasonable to expect a limit on the accuracy with which information can be reliably transmitted, however it is not accuracy that is limited but rather the rate at which information can be transmitted error free.

The codes referred to in the channel coding theorem do not prevent the occurrence of errors but rather allow their presence to be detected and corrected. As such the codes are known as *error-detecting* and *error-correcting codes* or for short *error-control codes*. Error-control codes fall into the categories of block codes and convolutional codes. We consider mainly block codes, convolutional codes are considered in Chapter 8. Before introducing block codes it is useful to consider the digital communication channel in general and then from the point of view of error-control codes.

1.1 The digital communication channel

The phrase *communication channel* is used here in a wide sense to describe any electronic system involving the transfer of information, and not just telecommunication systems. For example the transfer of data between the main memory of a computer and a data-storage device can be viewed as a communication system or subsystem. Applications of error-control codes tend to fall into the categories of digital telecommunication systems and data-storage systems. The main body of the theory of error-control codes, namely the construction of codes, encoding, decoding and performance evaluation, can be formulated without reference to the applications.

22/05/2023 11:58

Figure 1.1 shows a block diagram of a communication system. The *information source* provides information, in either a digital or analogue form, to the system. The information can be a message or data from some other system or person. The *source encoder* generates a binary signal that gives an efficient representation of the source information. This may involve the use of codes, other than error-control codes, that minimize the number of bits needed to represent each message and allow the message to be uniquely reconstructed by the *source decoder*. If the output from the information source is in an analogue form, then source encoding needs to be preceded by analogue-to-digital conversion.

The *channel encoder* carries out error-control coding for the purpose of protecting information against errors incurred as it progresses through the noisy channel. This is achieved by including additional information such that the *channel decoder* is able to accurately recover the source information despite the presence of errors. The transmission of information into the *channel* is performed by the *modulator*. In a telecommunication system the channel could typically be a wire link, a microwave link, a satellite link or some other type of link. The channel output feeds into the *demodulator* which carries out the inverse operation of the modulator, so producing a stream of bits from the received signal. The source and the channel encoders along with the modulator form the *transmitter*, whilst the demodulator and the source and the channel decoders form the *receiver* within the system. In a data storage system the modulator, the channel and the demodulator can be thought of as the writing unit, the storage medium and the reading unit respectively. The reconstruction of the source information by the source decoder is the last stage of the communication process, beyond this lies the *information user* which hopefully

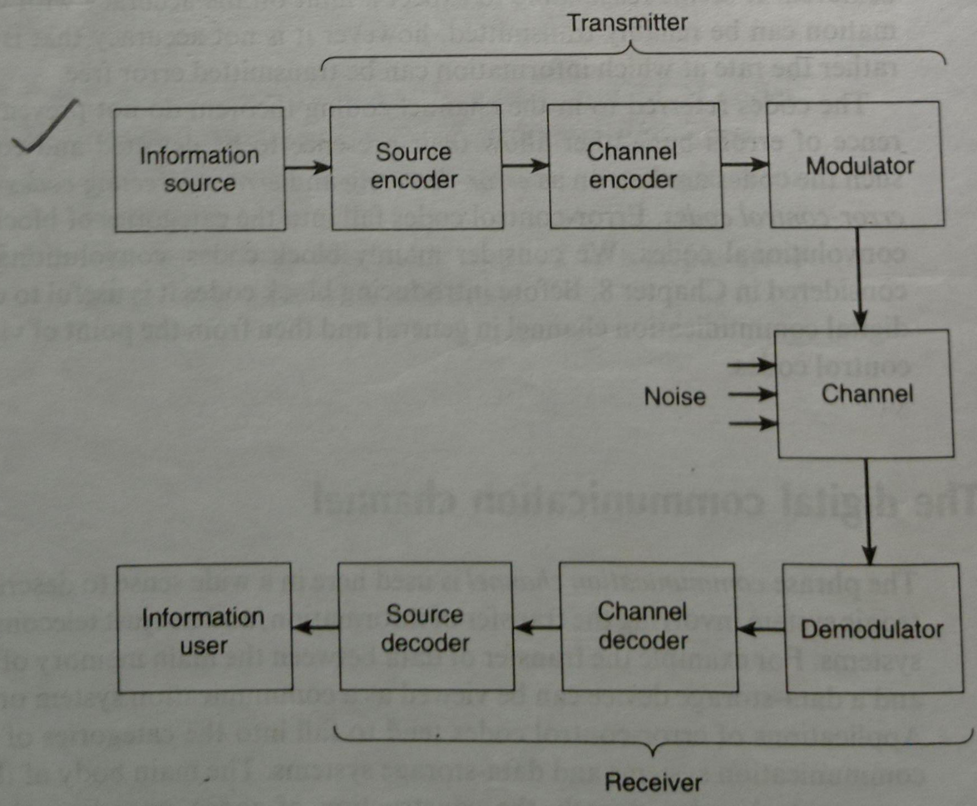

Fig. 1.1 Block diagram of a communication system

accurately receives information generated at the source. Note that the nature and contents of the information is of no importance to the communication system, which serves solely to enable communication.

With regard to error-control coding the communication system shown in Fig. 1.1 can be simplified to that shown in Fig. 1.2. Here the *digital source* combines the information source and the source encoder, and the *digital sink* combines the source decoder and the information user. The channel now includes the modulator and demodulator, and the channel encoder and channel decoder are now referred to simply as the *encoder* and the *decoder* respectively. The channel input is a stream of binary bits with 'values' 0 or 1, and we no longer think of noise occurring within the channel but rather the occurrence of *bit errors*, so that 0 and 1 become 1 and 0 respectively. The probability of an error can be determined from the characteristics of the modulator and the demodulator along with the statistical nature of the noise.

Of particular importance is the *binary symmetric channel* in which the probabilities of bits 0 and 1 incurring errors are equal. Figure 1.3 shows the transitions that can occur in the binary symmetric channel, the probability of a bit incurring an error is p and is referred to as the *bit-error probability* or the *transition probability*. The probability of a bit being received error free is $1-p$. Errors occur randomly within the binary symmetric channel, so whether a bit incurs an error is independent of whether other bits incur errors. Such a channel with *random errors* is known as a *random-error channel*, codes developed for dealing specifically with random errors are called *random-error-control codes*. If errors have a tendency to occur in groups or bursts then the channel is called a burst-error channel. We assume the channel to be binary symmetric and we will be considering random-error-control codes.

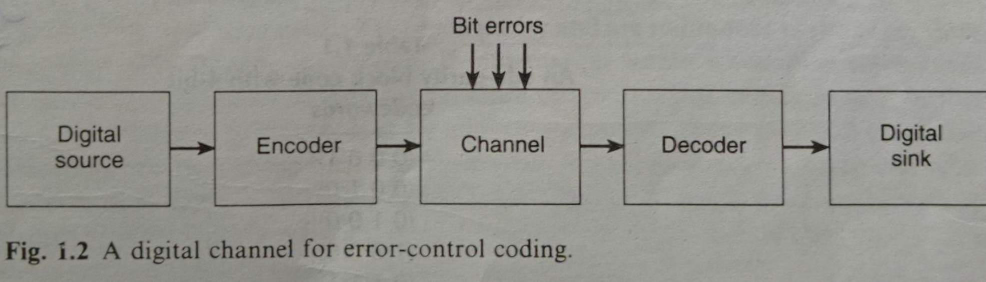

Fig. 1.2 A digital channel for error-control coding.

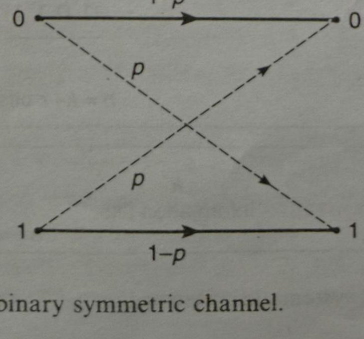

Fig. 1.3 Transitions in the binary symmetric channel.