Channel coding

Haim Permuter

I. Introduction

Shannon [1] has considered the channel coding problem as depicted in Fig. 1.

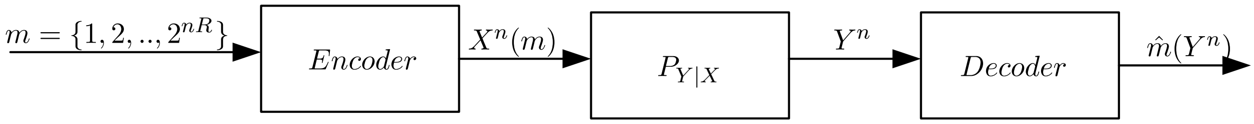

Fig. 1. Channel coding setting.

Prior to Shannon results, it was belived that the error probability of the channel communication in Figure 1, grows as R grows, where R is the rate transmitted through the channel, i.e., the number of bits transmitted through the channel per one usage of the channel. According to Shannon theorem, as long as we allow a delay such that the encoding is done in blocks of size n, the error probability is arbitrary low for $R \leq C$ and is 1 for $R > C$, where C is the channel capacity. This is illustraed in Figure 2.

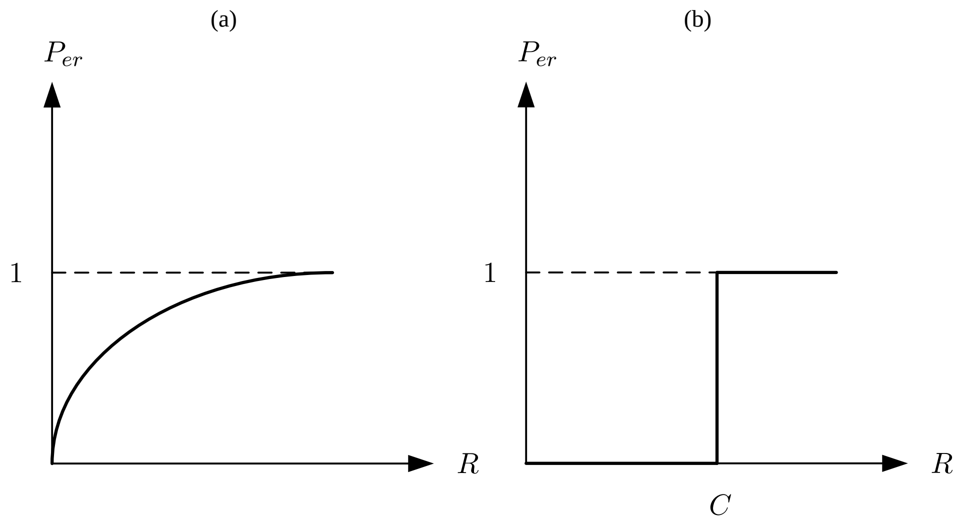

Fig. 2. (a) $P_{er}(R)$ as it was believed prior to Shannon theorem (b) $P_{er}(R)$ as derived from Shannon's theorem on capacity of channels

II. Problem Definition

In this section we present the formal definition of the channel coding problem.

Definition 1 (Code) An $(n, 2^{nR})$ code for the channel $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ consists of the following:

1) An index message $(1, \ldots, 2^{nR})$
2) An encoding function

$$f : \{1, 2, \ldots, 2^{nR}\} \to \mathcal{X}^n, \tag{1}$$

yielding codewords $x^n(1), x^n(2), \ldots, x^n(2^{nR})$. The set of codewords is called the *codebook*.
3) A decoding function

$$g : \mathcal{Y}^n \to \{1, 2, \ldots, 2^{nR}\}, \tag{2}$$

which is a deterministic rule that assigns a guess to each possible received vector.

Definition 2 (Maximal probability of error) The maximal probability of error, $P_{\max}$, for an $(n, 2^{nR})$ code is defined as:

$$P_{\max} = \max_m P(M \neq \hat{M} | M = m) \tag{3}$$

Definition 3 (Average probability of error) The average probability of error, $P_{er}^{(n)}$, for an $(n, 2^{nR})$ code is defined as:

$$P_{er}^{(n)} = \Pr\{M \neq \hat{M}\} \tag{4}$$

Definition 4 (Achievable rate) the rate R is achievable if there exists a sequence of $\{2^{nR}, n\}$ codes such that:

$$\lim_{n \to \infty} P_{er}^{(n)} = 0 \tag{5}$$

Definition 5 (Capacity) Capacity, which we denote by C, is the suprimum over all achievable rates.

III. Main Result

The main result on channel coding presented by Shannon [1] is given in Theorem 1 .

Theorem 1 (Channel capacity [1]) The capacity of a discrete memoryless channel is given by

$$C = \max_{P_X} I(X; Y) \tag{6}$$

where P_X is a distribution on the input alphabet $\mathcal{X}$ and $I(X; Y)$ is the mutual information.

References

[1] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423 and 623–656, 1948.