Introduction to Coding Theory

— Notes —

2 Shannon's Theorem

2.1 Introduction

Codewords are elements of $\mathbb{F}_2^n$. Random **noise** is added to the codewords view vector addition. The resulting vector may result in **errors** when decoded by the decoder.

Example of a situation where codes are used. Shows that if given infinite time, then can decrease chance of error to arbitrarily small. However, Shannon's theorem shows that you can still get arbitrarily small error rate even in finite situation.

Definition. If a code C is used consisting of words of length n, then

$$R := n^{-1} \log_2 |C|$$

is called the **information rate** of the code.

Definition. For $x, y \in \mathbb{F}_2^n$, the **Hamming distance** is

$$d(x, y) := \{i : x_i \neq t_i\}$$

2.2 Shannon's Theorem

There is probability p that a symbol is recieved in error, and probability $q := 1 - p$ that not. Use code word C consisting of M words of length n, each word occuring with equal probability. If $x_1, \ldots, x_M$ are the codewords and we use maximum-likelihood-decoding, let P_i be hte probability of making an incorrect decision given that x_i is transmitted. In that case, the probability of incorrect decoding of a received word is

$$P_C := M^{-1} \sum_{i=1}^{M} P_i$$

Define

$$P^*(M, n, p) := \min \{P_C : C \text{ a codeword of } M \text{ words of length } n \}$$

Theorem. (Shannon 1948) If $0 < R < 1 + p \log p + q \log q$ and $M_n := 2^{[Rn]}$ then $P^*(M_n, n, p) \to 0$ if $n \to \infty$.

Note that all logs are base 2. For $\epsilon > 0$ and n sufficiently large, there is a code C of length n with rate nearly 1 and such taht $P_C < \epsilon$.

Definition. The probability of an error pattern with w errors is $p^w q^{n-q}$ (depends on w only). The probability of receiving y given that x is transmitted, denoted $P(y|x)$, is equal to $P(x|y)$.

3 Linear Codes