1

1.1 Definition: Code

A code C of block length n over a finite alphabet Σ is any subset of Σ^n.

$$C \subseteq \Sigma^n$$

"the set of all possible codewords"

e.g. $\Sigma = \{0, 1\}$, $n = 5$, $C = \{00000, 11111, 00001\}$

1.2 Definition: Dimension of a Code

Given a code $C \subseteq \Sigma^n$, C has dimension k defined by:

$$k = log_{|\Sigma|}|C|$$

"n is the size of any codeword"

"k is the size of the decoded codeword"

Note: $k \leq n$

e.g. $\Sigma = \{0, 1\}$, $n = 5$, $C = \{00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111\}$ then, $k = log_2(8) = 3$

1.3 Definition: Rate of a code

Given a code $C \subseteq \Sigma^n$ with dimension k, C has rate R defined by:

$$R = \frac{k}{n}$$

"R is the ratio of non-redundent bits, higher is better, lower means more rendency"

1.4 Definition: Hamming Distance

The Hamming Distance between two equal length strings is the number of elementwise differences.

$$d_H = |\{i \mid x_i \neq y_i\}|$$

e.g. $d_H(bbb, aaa) = 3$

e.g. $d_H(xyz, abc) = 3$

1.5 Definition: Minimum distance of a code

Given a code $C \subseteq \Sigma^n$, C's minimum distance d is the smallest distance between any two codewords in C.

$$d = min\{d_H(i, j) \mid i, j \in C, i \neq j\}$$