Basic Definitions of Codes

The Hamming distance between two words $x, y \in \{0,1\}^n$ is the number of coordinates in which $x$ and $y$ differ. The Hamming distance will be denoted by $d_H(x, y)$. The Hamming distance is a metric as it satisfies the following three metric properties. For all $x, y, z \in \{0,1\}^n$,

1. Non-negativity: $d_H(x, y) \geq 0$ and equality if and only if $x = y$.
2. Symmetry: $d_H(x, y) = d_H(y, x)$.
3. The triangle inequality: $d_H(x, y) \leq d_H(x, z) + d_H(z, y)$.

The Hamming weight of a word $x \in \{0,1\}^n$, denoted by $w_H(x)$, is the number of nonzero entries in $x$. For all $x, y \in \{0,1\}^n$, $d_H(x, y) = w_H(x - y)$, and $w_H(x) = d_H(0, x)$, where $0$ is the all-zero vector.

A code is a nonempty subset $C$ of size $M$ of $\{0,1\}^n$, where $n$ is called the code length, $M$ is the code size, and the code is denoted by $(n, M)$. The dimension of the code $C$ is defined by $k = \log_2 M$, the rate of the code is $R = k/n$, and the redundancy of the code is $r = n - k = n - \log_2 M$. The elements of the code are called codewords.

The minimum distance of the code $C$, denoted by $d$, is the minimum Hamming distance between any two distinct codewords of $C$. That is,

$$d = \min_{c_1, c_2 \in C, c_1 \neq c_2} d_H(c_1, c_2).$$

We denote such a code by $(n, M, d)$.

**Example 1.**

1. The binary repetition code: For all $n \geq 1$, the binary repetition code is $C_n^{rep} = \{0^n, 1^n\}$.

For example, $C_5^{rep} = \{00000, 11111\}$. The length of the code $C_n^{rep}$ is $n$, its size is $M = 2$, the dimension is $k = 1$, the rate is $R = 1/n$, and the redundancy is $r = n - 1$. The minimum distance of the code is $n$. 

2. The binary parity code: For all $n \geq 1$, the binary parity code is

$$C_{\text{par}}^n = \{x \in \{0, 1\}^n \mid w_H(x) \text{ is even}\}.$$  

For example, $C_{\text{par}}^3 = \{000, 011, 101, 110\}$. The length of the code $C_{\text{par}}^n$ is $n$, its size if $M = 2^{n-1}$, the dimension is $n - 1$, the rate is $R = (n - 1)/n = 1 - 1/n$, and the redundancy is $r = 1$. The minimum distance is 2.

Communication Channel and Error-Correcting Codes

A communication system is a model for transmitting information from a source to a destination through a channel. The communication can be in the space domain to model transmission from one location to another or in the time domain for storing data at one point and retrieving it at later point.

Usually, the channel introduces errors in the transmitted data, where typical errors can be substitution of symbols, insertions, deletions, erasures and more. Hence, the user information $u$ is encoded using an encoder of some code to form a codeword $c$ that will be transmitted over the channel. The channel’s output, denoted by $y$, is a noisy version of $c$ and will be the input for the decoder of the code, while the goal is to recover the transmitted word $c$ and the information $u$.

![Communication channel](image)

Figure 1: Communication channel.

Assume we use an $(n, M)$ code $C$ to transmit over some channel. This process is described in the following steps.

1. An encoder to the code $C$ is a mapping $E_C : \{1, \ldots, M\} \to C$ which maps the user information $u$ into a codeword $c \in C$. Typically, when $M$ is a power of 2 and $k = \log_2 M$ the encoder can be denoted by $E_C : \{0, 1\}^k \to C$, so the user input is a word of $k$ bits.

2. Given the user information $u$, its encoded codeword $c = E_C(u)$ is transmitted over the channel, and the resulting channel’s output is a noisy word $y \in \{0, 1\}^n$ which is fed to a channel decoder.

3. A decoder to the code $C$ is a mapping $D_C : \{0, 1\}^n \to C$, which receives the channel’s output $y$ and outputs a codeword $\hat{c}$ (and thus also the information $\hat{u}$), with the aim of having $\hat{c} = c$ and $\hat{u} = u$.

The success of the decoder depends on the code we use and the number of errors caused by the channel.
The difference word $e = y - c$ is called the error word. If for all channel input $c$ and channel output $y$, it holds that $w_H(e) = w_H(y - c) \leq t$, for some fixed value $t$, then it is said that channel causes at most $t$ errors.

The nearest-codeword decoder for an $(n, M)$ code is a mapping $D_{C}^{NC} : \{0,1\}^n \rightarrow C$, where the output of every $y \in \{0,1\}^n$ is the closest codeword $c \in C$, in Hamming distance, to $y$. That is,

$$D_{C}^{NC}(y) = c,$$

where for every $c' \in C$, $d_H(y, c) \leq d_H(y, c')$. In case there is more than one such a codeword, then the decoder outputs one of them arbitrarily.

A code $C$ is said to be a $t$-error-correcting code if its nearest-codeword decoder can correct any $t$ or less errors which are caused by the channel.

Example 2.

1. Consider the repetition code $C_5^{rep} = \{00000, 11111\}$. An example for an encoder to the code $C_5^{rep}$ is the mapping $E_{C_5^{rep}} : \{0,1\} \rightarrow C_5^{rep}$, which is defined as follows:

$$E_{C_5^{rep}}(0) = 00000, E_{C_5^{rep}}(1) = 11111.$$

The nearest-codeword decoder of the code $C_5^{rep}$ is the mapping $D_{C_5^{rep}}^{NC} : \{0,1\}^5 \rightarrow C_5^{rep}$, which is defined as follows: For every $y \in \{0,1\}^5$,

$$D_{C_5^{rep}}^{NC}(y) = \begin{cases} 00000 & \text{if } w_H(y) \leq 2, \\ 11111 & \text{if } w_H(y) > 2. \end{cases}$$

2. Consider the binary parity code $C_3^{par} = \{000, 011, 101, 110\}$. An example for an encoder to the code $C_3^{par}$ is the mapping $E_{C_3^{par}} : \{0,1\}^2 \rightarrow C_3^{par}$, which is defined as follows: for all $u = (u_0, u_1) \in \{0,1\}^2$,

$$E_{C_3^{par}}((u_0, u_1)) = (u_0, u_1, u_0 + u_1).$$

If the transmitted word is $c = E_{C_3^{par}}((0,0)) = (0,0,0)$ and one error occurred by the channel, to produce the output $y = (0,1,0)$, then the output of the nearest-codeword decoder of the code $C_3^{par}$ can be any of the following three codewords: $\{(0,0,0), (0,1,1), (1,1,0)\}$.

\[3\]

Theorem 1. An $(n, M, d)$ code $C$ is a $t$-error-correcting code if $t \leq \lfloor \frac{d-1}{2} \rfloor$.

Proof. Based upon Proposition 1.3. Given in class.

Theorem 2. For any $(n, M, d)$ code $C$, it holds that

$$M \leq \frac{2^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}}.$$
Proof. Based upon Theorem 4.3. Given in class.

An *erasure* is the event where some of the entries in the transmitted codeword $c$ are erased, so the channel output $y$ satisfies $y \in \{0, 1, ?\}^n$. It is said that the channel *causes at most some $t$ errors and $e$ erasures* in the channel output has at most $t$ errors and at most $e$ erasures with respect to the channel input $c$. A code is called *$t$-error-$e$-erasure-correcting code* if it can correct any $t$ or less errors and $e$ or less erasures which are caused by the channel.

**Theorem 3.** An $(n, M, d)$ code $C$ is a $t$-error-$e$-erasure-correcting code if

$$2t + e \leq d - 1.$$  

Proof. Based upon Theorem 1.7. Not given in class.

**Problem 1.** Let $C_1$ be an $(n_1, M_1, d_1)$ code. Define the code $C_2$ by

$$C_2 = \{(c, e) \mid c \in C_1\}.$$  

1. What are the length, size, dimension, rate, redundancy, and minimum distance of the code $C_2$?

   **Solution:**

   (a) $n_2 = 2 \cdot n_1$
   
   (b) $M_2 = M_1$
   
   (c) $k_2 = \log_2 M_2 = \log_2 M_1$
   
   (d) $R_2 = \frac{k_2}{n_2} = \frac{\log_2 M_1}{2n_1}$
   
   (e) $r_2 = n_2 - k_2 = 2 \cdot n_1 - \log_2 M_1$
   
   (f) $d_2 = 2 \cdot d_1$

2. Assume $D_{C_1} : \{0, 1\}^{n_1} \rightarrow C_1$ is a decoder for $C_1$ which can correct any $t_1$ errors and $t_2$ erasures provided that $2t_1 + t_2 \leq d_1 - 1$. Show how to use the decoder $D_{C_1}$ in order to construct a decoder, $D_{C_2} : \{0, 1\}^{2n_1} \rightarrow C_2$, that can correct $d_1 - 1$ errors for the code $C_2$?

   **Solution:** Every bit has two copies, so we can output a word of length $n$ by majority over the two copies for each bit and in case of disagreement, we output an erasure symbol. Then, by showing that in the majority word the number of errors $t$ and number of erasures $e$ satisfies, $2t + e \leq d_1 - 1$, the decoder $D_{C_1}$ will be successful.