1 Introduction to Coding Theory

Coding theory and error-correcting codes were developed to enable the reliable transmission of messages over noisy communication channels. One important distinction is that we are assuming the noise is *non-adversarial*, that is, the codes we consider are not made to be cryptographically secure. Rather, the codes protect against random (unintentional) error. They are used in the classical setting, for example in CDs (if anyone still uses CDs) to prevent data loss in the event of a scratch and long-distance space communications with rovers and satellites. An interesting aspect of coding theory that we will not cover is that different codes have been optimized for different noise models.

Error-correcting codes are important for the practical implementation of quantum computers because current physical implementations of quantum computers are plagued by *quantum decoherence*. That is, the qubits are difficult to fully isolate from their environment and thus become entangled with their surroundings, leading to noisy computations. For now, we will forget about quantum computing and plunge into the theory of error-correcting codes.

1.1 Preliminaries

As was mentioned, we consider the scenario that we are transmitting a message over a noisy communication channel. More specifically, we will look at *binary symmetric channels*.

Definition 1 (Binary Symmetric Channel)**.** *A binary symmetric channel is a classical channel that can transmit a string of 0's and 1's. If a bit b is sent, b will be flipped to $\neg b$ with probability p, and b will be transmitted correctly with probability $1-p$ where $p < \frac{1}{2}$.*

This type of channel is *binary* because we are transmitting bits, and it is *symmetric* because there is an equal probability of a 0 flipping to a 1 and the reverse. Note that if our binary symmetric channel flips bits with probability $p > 1/2$, we could easily create a channel with $p < 1/2$ by negating every bit on the receiving or sending end. Additionally, note that if $p = 1/2$, it is information-theoretically impossible to recover the message, so we don't consider this case and frankly it is dubious to even call that a communication channel.

In the following subsections we will investigate how to mitigate the information loss from these random errors in binary symmetric channels where $p < 1/2$.

1.2 Encoding and Decoding

The basic idea behind error-correcting codes is that we will systematically introduce redundancy to the message we want to send; this process is called *encoding*.

Definition 2 (Message, encoding)**.** *We will denote our message* m *as* $m_0m_1m_2\dots m_{k-1}$ *where* $m_i \in \{0,1\}$ *for all* $0 \leq i \leq k-1$*. Next, we will denote the encoding of our message* m*, called a codeword,* $E(m) = u_0u_1u_2\dots u_{n-1}$ *where* $n > k$ *and* $u_i \in \{0,1\}$ *for all* $0 \leq i \leq n-1$*.*