Quantum Information Theory

quinten tupker

January 22 2021 - January 22, 2021

Introduction

These notes are based on the course lectured by Professor S Strelchuk in Lent 2020. This was lectured online due to measures taken to counter the spread of Covid-19 in the UK. These are not necessarily an accurate representation of what was lectures, and represent solely my personal notes on the content of the course, combinged with probably, very very many personal notes and digressions... Of course, any corrections/comments would be appreciated.

Information theory is the theory of information storage and transmission. It provides the theoretical limits on what is possible with information technologies in much of our world, and a framework to study many other fields, such as animal communication as well. This is the quantum qersion of that theory.

1 Classical Information Theory

We begin by observing that information is closely related to uncertainty. In particular, what might be able to say it is the opposite of uncertainty, and so then, it is no surprise that we build our theory of information using concepts from probability theory. As such we define

Definition 1. The **surprisal** of random variable X taking values in discrete finite **alphabet** J according to distribution $p(x)$ is

$$\mathcal{I}(x) = -\ln(p(x))$$

Definition 2. The **Shannon entropy** of a random variable X is

$$H(X) = -\sum_{x\in J} p(x)\ln(p(x))$$

This may appear to be a somewhat arbitrary definition, but it has a strong theoretical basis given that

Theorem 1. The **Shannon Source Coding Theorem** states (informally) that the limit that information can be compressed so that it can be reliably retrieved is the Shannon entropy of the source.

Here a basic example of a source is a **memoryless source** which is an object producing a sequence of signals, but since it is memoryless, each signal is completely independent from any other, so $\mathbb{P}(u_1, \ldots, u_n) = \mathbb{P}(u_1) \ldots \mathbb{P}(u_n)$. It is also known as an **i.i.d. information source**.

But how do we actually compress information? Conceptually there are two ways

- a **variable length encoding** stores higher probability signals in shorter codes, and lower probability signals in longer codes.
- a **fixed length encoding** stores higher probability signals in unique fixed length codes, and lower probability signals in the same fixed code.

Example 1. An example of a fixed length code for the numbers $1, \ldots, 8$ are their binary representations, but if we also know that $p(1, \ldots, 8) = 1/2, 1/4, 1/8, 1/16, 1/64, 1/64, 1/64, 1/64$ then the code $C(1, \ldots, 8) = 0, 10, 110, 1110, 111100, 111101, 111110, 111111$ has an average length 2 compared to the fixed length of 3. Furthermore, the Shannon entropy of this source is 2 as well, so this is maximally efficient.

1.1 Classical Data Compression

Let's start making the definitions necessary to formalise compression.

Definition 3. A **compression map** is a map $C^n : u^{(n)} = (u_1, \ldots, u_n) \mapsto x(x_1, \ldots, x_{nR})$ sending a **message** u to a **code** x.

Definition 4. A **decompression map** D^n sends $D^n : x \in \{0,1\}^{\lceil nR \rceil} \mapsto u'^{(n)}$ with probability $\mathbb{P}(u^{(n)}|x)$.

Definition 5. A **code** of rate R and blocklength n is the triple (C^n, D^n, R).

Here we can compute the probability of error as

$$P_{av}^{(n)}(C_n) = \sum_{u^{(n)} \in J^n} \mathbb{P}(u^{(n)}) \mathbb{P}(D^n(C^n(u^{(n)})) \neq u^{(n)}).$$