PHYS 7895: Quantum Information Theory Fall 2015

Lecture 1 — August 24, 2015

Prof. Mark M. Wilde *Scribe: David Kekejian*

1 Introduction to Quantum Information Theory

Why study Quantum Information Theory? To discover ultimate limits on communication and how to achieve them. Also, quantum strategies for communication allow for sending data at higher rates than can exclusively classical strategies.

2 Main concepts in QIT

Let us suppose a sender Alice wants to send a message to a receiver Bob. What is the main procedure of sending this message?

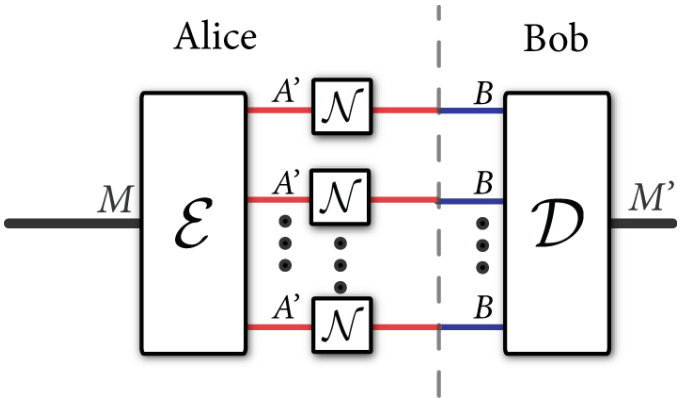

Figure 1: The most general protocol for classical communication over a quantum channel $\mathcal{N}$. Alice selects some message M and encodes it as a quantum codeword for input to many independent uses of the noisy quantum channel. Bob performs some quantum measurement over all of the channel outputs to determine the message that Alice transmits. $\mathcal{E}$ represents the encoding and $\mathcal{D}$ represents the decoding.

Alice encodes the message as a quantum state and sends this over many uses of a noisy quantum channel. The noise affects the encoded information and could result in a loss of information. In this procedure and throughout the course, we are assuming that both Alice and Bob have perfect encoders and decoders that can perform any quantum operations. We are also assuming that the channels are i.i.d. (Independent and Identically distributed). Independent means that the channels are acting independently and identically distributed means that the noise is acting in the same way on each quantum system. If the number of uses of the channel is large enough, such that we can assume the law of large numbers comes into play, then we can argue about what communication rates are achievable using the channel many times.

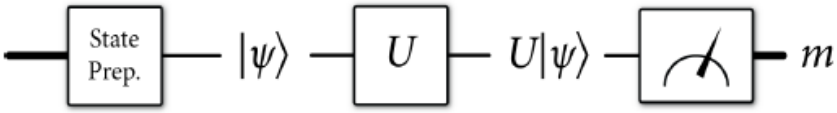

Figure 3.1: All of the steps in a typical noiseless quantum information processing protocol. A classical control (depicted by the thick black line on the left) initializes the state of a quantum system. The quantum system then evolves according to some unitary operation (described in Section 3.3). The final step is a measurement that reads out some classical data m from the quantum system.

In the next few weeks we will be discussing the detail mathematics about what is going inside the boxes in Figure 2 (preparation, evolution, and measurement).

Final Project Ideas

1. *Classical capacity* is the maximum rate at which classical data can be sent over the channel with arbitrarily small error, when allowing for many uses of the channel. Examples of projects: What if noise is not i.i.d.? What rates of communication can we achieve with a limited number of channel uses?

2. *Quantum capacity* is the highest rate at which quantum information can be communicated over many independent uses of a noisy quantum channel, such that the error becomes arbitrarily small. Examples of projects: Superactivation would be interesting—it is a phenomenon in which two different quantum channels which individually have zero quantum capacity can have a non-zero capacity when used together.

3. *Private capacity* includes the encryption of private messages and secret communication.

4. *Trade-offs* which includes having both classical and quantum data transmissions.

5. *Quantum Key distribution*: device independence, which means the demand for a protocol to be secure even if you do not trust the device that you are working with. For example, the device could be made by the adversary, and we would like to still have secrecy in such a scenario.

6. *Intersection of quantum information theory with other areas of physics*: for example, thermodynamics, quantum gravity, condensed matter physics, etc...