Applied Physics 150a: Homework #1

(Dated: October 16, 2014)

Due: Thursday, October 23rd, anytime before midnight. There will be an "INBOX" outside my office in Watson (Rm. 266/268).

1. **(20 points) Shor's algorithm**

   Read through the notes in Ref.[1] on the Parity Problem and Shor's algorithm for factoring numbers.

   (a) Write out the quantum network for a circuit that solves the quantum parity problem, providing a description for each element used in the quantum network.

   (b) Explain how the quantum parity circuit utilizes an ancillary qubit to "kick back a phase" to the input qubits.

   (c) How does Shor's algorithm make use of a similar "phase kick-back" to solve the factoring problem? Draw the relevant part of the quantum network, and explain.

2. **(20 points) Building on the no-cloning theorem**

   (a) The *no-deleting* theorem of quantum mechanics states that given two identical copies of an arbitrary quantum state, it is impossible to delete (reset) one of the copies. Prove the no-deleting theorem for an arbitrary qubit state.

   (b) The no-cloning theorem has a counterpart for mixed states called the *no-broadcast* theorem. The no-broadcast theorem addresses the question, "Are there any physical means for broadcasting an unknown quantum state onto two separate quantum systems?" The pure state no-cloning theorem prohibits broadcasting pure quantum states as the only way to broadcast a pure state $|\Psi\rangle$ is to put it into state $|\Psi\rangle \otimes |\Psi\rangle$, which is simply to clone it. Things are more complicated when the states are mixed. To understand why take a look at the paper by Barnum, et al. [2]. Provide a brief synopsis of the no-broadcast theorem proof given by Barnum and colleagues, and discuss the implications of this theorem to quantum information processing and quantum communication.

3. **(20 points) Quantum limits to linear amplifiers**

The above no-cloning theorem for quantum states is intimately tied to the fundamental limits of precision measurement. If one would like to measure things down at the quantum level, then typically we need an *amplifier* to convert the small quantum-level signal up to a much larger signal that can be read out with large signal-to-noise, even in the presence of other technical noise. As put by Carlton Caves in his classic paper on quantum limits to linear amplifiers [3], "...the last essential quantum mechanical stage of a measuring apparatus is a high-gain amplifier; it produces an output that we can lay our grubby, classical hands on."

(a) Take a look at Ref. [3]. Set up the problem, and define (you needn't derive) the quantum limits of both a phase-insensitive and phase-sensitive linear amplifier in terms of its added noise.

(b) How are the no-cloning theorem and the quantum limits to linear amplifiers related? Explain.

(c) Bonus (5 points): If one had a perfect amplifier of optical photons explain how this could be used to perform faster than light (superluminal) communication [You might want to do a little digging in the literature for inspiration].

---

[1] E. Knill, R. Lafflame, H. Barnum, D. Dalvit, J. Dziarmaga, J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola, and W. H. Zurek, arXiv:0207171 (2008).

[2] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[3] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).