COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the semester will be dropped from your final grade.

Problems:

1. (2 points) **Copying qubits.** Consider a unitary operation U that can copy the eigenstates of the standard basis. That is, U is a 4×4 unitary matrix such that $U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and $U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$.

   (a) Does such a U exist? If so, justify; if not, prove why not.

   (b) Assume such a U does exist. Can you infer what vector it sends $|-\rangle\,|0\rangle$ to? Give a formal statement for the version of the "no-cloning theorem" that you have just proved.

   (c) Suppose that $\{|\psi_1\rangle, |\psi_2\rangle\}$ are qubit states such that $0 < |\langle\psi_1|\psi_2\rangle| < 1$. Prove that there does not exist an U that satisfies $U(|\psi_i\rangle\,|0\rangle) = |\psi_i\rangle\,|\psi_i\rangle$ for $i \in \{1, 2\}$. *[Hint: this does not use the previous questions. Think about what you know of unitary matrices]* Deduce a second formal statement for a "no-cloning theorem", that matches what you just proved.

2. (4 points) **The EPR pair.** Recall the definition of the EPR pair,

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\,\big)\ .$$

   Prove rigorously that there does not exist two single-qubit states $|\psi\rangle$ and $|\phi\rangle$ such that $|\mathrm{EPR}\rangle = |\psi\rangle \otimes |\phi\rangle$. *[Hint: Reason by contradiction. Expand everything in the standard basis.]*