COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 2

This exercise sheet is designed to help you review the concepts discussed in the lecture and explore some additional interesting results that were not covered in the lecture. Solutions to selected exercises will be provided after the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. **A cloning map**
   In this exercise we verify that the map T defined in Example **??** is a valid quantum map.

   (a) Start with a simple "sanity check": verify that each of the four matrices ρ_0, ρ_1, ρ_+ and ρ_- is a valid density matrix.

   However, this is not enough: for example, these conditions are satisfied by the "optimal cloning map" $|\psi_\$\rangle\langle\psi_\$| \mapsto |\psi_\$\rangle\langle\psi_\$| \otimes |\psi_\$\rangle\langle\psi_\$|$, but we know that there exists no such map! To see that T is a well-defined map, we verify that it can be implemented by (i) adding two ancilla qubits in state $|00\rangle_{BC}$, (ii) a unitary transformation, and (iii) a tracing-out operation.

2. Consider the following map V, where as usual $|\mathrm{EPR}\rangle$ is an EPR pair.

$$|0\rangle_A |00\rangle_{BC} \mapsto \frac{2}{\sqrt{6}} |00\rangle_{AB} |0\rangle_C + \frac{1}{\sqrt{3}} |\mathrm{EPR}\rangle_{AB} |1\rangle_C \ ,$$
$$|1\rangle_A |00\rangle_{BC} \mapsto \frac{1}{\sqrt{3}} |\mathrm{EPR}\rangle_{AB} |0\rangle_C + \frac{2}{\sqrt{6}} |11\rangle_{AB} |1\rangle_C \ .$$

   Check that the two states on the right-hand side, call them $|v_0\rangle$ and $|v_1\rangle$, are orthonormal. Using Remark **??** this shows that it is possible to extend V to a valid unitary operation on the entire 3-qubit space $\mathbb{C}^8$.

3. Show that the map T is identical to the composition of adding two ancilla qubits in state $|00\rangle_{BC}$, applying V, and tracing out the third qubit. That is, for all states $|\psi\rangle$,

$$T(|\psi\rangle\langle\psi|_A) = \mathrm{Tr}_C\big(V\big(\,|\psi\rangle\langle\psi|_A \otimes |00\rangle\langle 00|_{BC}\,\big)V^\dagger\big) \ .$$

This justifies that T is a valid quantum map, because it can be written as a sequence of three valid operations.