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. Exercises marked with * will have solutions provided after the exercise session, while those marked with ♦ will be the main focus during the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. (*) **Composing quantum maps**
   Show carefully that the composition of two quantum maps, each given as a sequence of (i) ancilla qubit preparation, (ii) unitary evolution, (iii) partial qubit trace out, is still a quantum map. In other words, show that a sequence of (i), (ii) and (iii) repeated twice can be "re-ordered" so that all the ancilla preparation come first and all the tracing out comes last, without changing how the map operates on any quantum state.

2. (*) **The depolarizing channel**
   The map $\mathcal{N}_{\text{depolarizing}}(\rho_A) = (1-p)\rho_A + \frac{p}{2}\mathbb{I}_A$ is called *depolarizing noise* with strength p. Find the Kraus operators for this channel, and then find a decomposition of it as a sequence of qubit addition, unitary and tracing out operations. *[Hint: remember the identity showing security of the quantum one-time pad!]*

3. (♦) **A cloning map**
   In this exercise, we verify that there exists a valid quantum map T from single-qubit quantum states to two-qubit density matrices that satisfies the following:

$$
\begin{aligned}
|0\rangle\langle 0| \mapsto \rho_0 &= \frac{2}{3}|00\rangle\langle 00| + \frac{1}{3}|\psi^+\rangle\langle\psi^+| \ , \\
|1\rangle\langle 1| \mapsto \rho_1 &= \frac{2}{3}|11\rangle\langle 11| + \frac{1}{3}|\psi^+\rangle\langle\psi^+| \ , \\
|+\rangle\langle +| \mapsto \rho_+ &= \frac{1}{12}\big(2|00\rangle + \sqrt{2}|\psi^+\rangle\big)\big(2\langle 00| + \sqrt{2}\langle\psi^+|\big) \\
&\quad + \frac{1}{12}\big(2|11\rangle + \sqrt{2}|\psi^+\rangle\big)\big(2\langle 11| + \sqrt{2}\langle\psi^+|\big) \ , \\
|-\rangle\langle -| \mapsto \rho_- &= \frac{1}{12}\big(2|00\rangle - \sqrt{2}|\psi^+\rangle\big)\big(2\langle 00| - \sqrt{2}\langle\psi^+|\big) \\
&\quad + \frac{1}{12}\big(2|11\rangle - \sqrt{2}|\psi^+\rangle\big)\big(2\langle 11| - \sqrt{2}\langle\psi^+|\big) \ ,
\end{aligned}
$$

   where we write $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

   (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.

(b) Consider the following map V.

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

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

(c) 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 $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$,

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

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

(d) Verify that for $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$,

$$\langle\psi|\,\langle\psi|\,T\big(\,|\psi\rangle\langle\psi|\,\big)\,|\psi\rangle\,|\psi\rangle \;=\; \frac{2}{3} \ .$$