COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 2

1. **Composing quantum maps**

   Suppose that we perform the following sequence of operations, starting with n qubits in state ρ: (a) add n_1 qubits in state $|0\rangle$; apply U_1 on $n+n_1$ qubits; trace out k_1 qubits, and (b) add n_2 qubits in state $|0\rangle$; apply U_2 on $n+n_1+n_2-k_1$ qubits; trace out k_2 qubits. Then we make the following observations. Firstly, the n_2 qubits at step (b) could have been added at the start of step (a); as long as they are not used until step (b) this does not make a difference. Secondly, the k_1 qubits can be traced out at the end of step (b); as long as they are not touched throughout step (b) then it does not make a difference when we trace them out. As a result, the combination of (a) and (b) can be described as (c) add n_1+n_2 qubits in state $|0\rangle$; apply U_1 on the first $n+n_1$ qubits, and U_2 on all qubits except the k_1 that will be traced out; trace out k_1+k_2 qubits. Since the middle part of (c) can be described as the application of a single, bigger unitary U (that is the composition of U_1 and U_2), we have obtained the required description.

2. **The depolarizing channel**

   Recall the identity we proved in the lecture of quantum one-time pad:

   $$\frac{1}{4}(\rho + X\rho X + Z\rho Z + XZ\rho ZX) = \frac{\mathbb{I}}{2},$$

   for every single-qubit mixed state ρ.

   Let $K_1 = \sqrt{1-3p/4}\mathbb{I}$, $K_2 = \sqrt{p}X/2$, $K_3 = \sqrt{p}Z/2$, and $K_4 = \sqrt{p}XZ/2$. Then it is easy to verify that

   $$\sum_{i=1}^{4} K_i^\dagger K_i = \mathbb{I},$$

   and

   $$\sum_{i=1}^{4} K_i \rho K_i^\dagger = (1-p)\rho + \frac{p}{2}\mathbb{I},$$

   for every single-qubit mixed state ρ, using the above identity.

   We can implement this channel on a register A by introducing three quantum qubits initialized as $|0\rangle_B |0\rangle_C |0\rangle_D$, applying the Hadamard gate H on registers B and C, applying the unitary $U_1 = (\sqrt{1-p}\,|0\rangle + \sqrt{p}\,|1\rangle)\langle 0| + (\sqrt{p}\,|0\rangle - \sqrt{1-p}\,|1\rangle)\langle 1|$ on register D, applying the unitary $U_2 = |11\rangle\langle 11|_{BD} \otimes Z_A + (\mathbb{I} - |11\rangle\langle 11|)_{BD} \otimes \mathbb{I}_A$ and the unitary $U_3 = |11\rangle\langle 11|_{CD} \otimes X_A + (\mathbb{I} - |11\rangle\langle 11|)_{CD} \otimes \mathbb{I}_A$, and finally tracing out the registers B, C and D.

3. **A cloning map**