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. **A cloning map**

   (a) Since each of the four matrices is expressed as a linear combination, with positive coefficients, of rank-1 projections, it is positive. It only remains to check that each of them has trace 1. For example, for ρ_+ the trace is

   $$\begin{aligned}\mathrm{Tr}(\rho_+) &= \frac{1}{12}\big(\|2\,|00\rangle + \sqrt{2}\,|\psi_{11}\rangle\,\|^2 + \|2\,|11\rangle + \sqrt{2}\,|\psi_{11}\rangle\,\|^2\big)\\ &= \frac{1}{12}(6+6) \;=\; 1\;.\end{aligned}$$

   Here for the second line we used that $|00\rangle$ and $|\psi_{11}\rangle$, and $|11\rangle$ and $|\psi_{11}\rangle$, are pairs of orthonormal vectors.

   (b) Using that $\langle 00|\,\psi_{11}\rangle = \langle 11|\,\psi_{11}\rangle = 0$ we verify that $\langle v_0|\,v_1\rangle = 0$, and moreover $\|\,|v_0\rangle\,\| = \|\,|v_1\rangle\,\| = 1$.

   (c) Let's do the verification for the case $|\psi\rangle = |+\rangle$. Then,

   $$\begin{aligned}T(|+\rangle\langle+|_A) &= \mathrm{Tr}_C\big(V\big(\,|+\rangle\langle+|_A \otimes |00\rangle\langle 00|_{BC}\,\big)V^\dagger\big)\\ &= \mathrm{Tr}_C\Big(\frac{1}{2}\big(\,|v_0\rangle + |v_1\rangle\,\big)\big(\,\langle v_0| + \langle v_1|\,\big)\Big)\\ &= \frac{1}{2}\Big(\big(\frac{2}{\sqrt{6}}\,|00\rangle + \frac{1}{\sqrt{3}}\,|\psi_{11}\rangle\,\big)\big(\frac{2}{\sqrt{6}}\,\langle 00| + \frac{1}{\sqrt{3}}\,\langle\psi_{11}|\,\big)\\ &\qquad + \big(\frac{1}{\sqrt{3}}\,|\psi_{11}\rangle + \frac{2}{\sqrt{6}}\,|11\rangle\,\big)\big(\frac{1}{\sqrt{3}}\,\langle\psi_{11}| + \frac{2}{\sqrt{6}}\,\langle 11|\,\big)\Big)\;.\end{aligned}$$

Here, for the third line we expanded using the definition of $|v_0\rangle$ and $|v_1\rangle$, and used that $\mathrm{Tr}_C(|0\rangle\langle 1|_C) = \mathrm{Tr}_C(|1\rangle\langle 0|_C) = 0$ to eliminate the cross terms. By re-arranging the constant coefficients you can verify that this equals ρ_+.