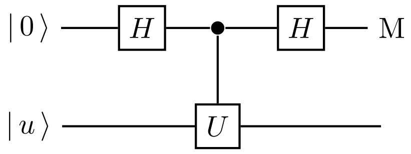
# C7.4 Introduction to Quantum Information
# Model Solutions

1. Consider the following quantum network composed of the two Hadamard gates, one controlled-$U$ operation and the measurement $M$ in the computational basis,



The top horizontal line represents a qubit and the bottom one an auxiliary physical system.

(a) [6 marks] Suppose $|\,u\,\rangle$ is an eigenvector of $U$, such that $U|\,u\,\rangle = e^{i\alpha}|\,u\,\rangle$. Step through the execution of this network, writing down quantum states of the qubit and the auxiliary system after each computational step. What is the probability for the qubit to be found in state $|\,0\,\rangle$?

Regardless the state of the auxiliary system, the probability $P_0$ for the qubit to be found in state $|\,0\,\rangle$, when the measurement $M$ is, can be written as

$$P_0 = \frac{1}{2}\left(1 + v\cos\phi\right),$$

where $v$ and $\phi$ depend on $U$ and on the initial state of the auxiliary system.

(b) [9 marks] Show that for an arbitrary pure state $|\,u\,\rangle$ of the auxiliary system the quantities $v$ and $\phi$ are given by the relation $ve^{i\phi} = \langle\, u\,|U|\,u\,\rangle$.

(c) [7 marks] Suppose the auxiliary system is prepared in a mixed state described by the density operator $\rho$,

$$\rho = p_1|\,u_1\,\rangle\langle\,u_1\,| + p_2|\,u_2\,\rangle\langle\,u_2\,| + ...... + p_n|\,u_n\,\rangle\langle\,u_n\,|,$$

where vectors $|\,u_k\,\rangle$ form an orthonormal basis, $p_k \geqslant 0$ and $\sum_{k=1}^{n} p_k = 1$. Show that

$$ve^{i\phi} = \mathrm{Tr}(\rho U).$$

(d) [3 marks] How would you modify the network in order to estimate $\mathrm{Tr}(\rho U)$? How would you estimate $\mathrm{Tr}\,U$?

**Solution:**

(a) Stepping through the execution of the network:

$$|\,0\,\rangle|\,u\,\rangle \overset{H}{\longrightarrow} \frac{1}{\sqrt{2}}\left(|\,0\,\rangle + |\,1\,\rangle\right)|\,u\,\rangle \xrightarrow{C-U} \frac{1}{\sqrt{2}}\left(|\,0\,\rangle|\,u\,\rangle + |\,1\,\rangle U|\,u\,\rangle\right) = \frac{1}{\sqrt{2}}\left(|\,0\,\rangle + e^{i\alpha}|\,1\,\rangle\right)|\,u\,\rangle$$
$$\overset{H}{\longrightarrow} \left[\frac{1+e^{i\alpha}}{2}|\,0\,\rangle + \frac{1-e^{i\alpha}}{2}|\,1\,\rangle\right]|\,u\,\rangle = e^{i\alpha/2}\left[\cos\frac{\alpha}{2}|\,0\,\rangle - i\sin\frac{\alpha}{2}|\,1\,\rangle\right]|\,u\,\rangle$$

The state just before the measurement can be written as

$$\left(\cos\frac{\alpha}{2}|\,0\,\rangle - i\sin\frac{\alpha}{2}|\,1\,\rangle\right)|\,u\,\rangle$$

since the global phase is irrelevant. [5 marks]
Therefore, the probability for finding the qubit in state $|\,0\,\rangle$ is

$$\cos^2\left(\frac{\alpha}{2}\right) = \frac{1}{2}\left(1+\cos\alpha\right). \qquad [1]$$

*Discussed in the lectures.*

(b) The combined state before the second Hadamard gate is:

$$\frac{1}{\sqrt{2}}\left(|\,0\,\rangle|\,u\,\rangle + |\,1\,\rangle U|\,u\,\rangle\right)$$

and after the Hadamard gate:

$$|\,0\,\rangle\left(\frac{|\,u\,\rangle + U|\,u\,\rangle}{2}\right) + |\,1\,\rangle\left(\frac{|\,u\,\rangle - U|\,u\,\rangle}{2}\right) \qquad \text{[1 mark]}$$

The probability $P_0$ is the squared modulus of the corresponding amplitude:

$$P_0 \;=\; \left(\frac{|\,u\,\rangle + U|\,u\,\rangle}{2}\right)^{\dagger}\left(\frac{|\,u\,\rangle + U|\,u\,\rangle}{2}\right) = \frac{1}{4}\left(2 + \langle\,u\,|U|\,u\,\rangle + \langle\,u\,|U^{\dagger}|\,u\,\rangle\right)$$

where we have made use of the unitarity of $U$:

$$\langle\,u\,|U^{\dagger}U|\,u\,\rangle = \langle u|u\rangle = 1 \qquad \text{[5 marks]}$$

Writing

$$\begin{aligned} ve^{i\phi} &= \langle\,u\,|U|\,u\,\rangle \\ ve^{-i\phi} &= \langle\,u\,|U^{\dagger}|\,u\,\rangle, \end{aligned}$$

the probability $P_0$ becomes

$$P_0 = \frac{1}{4}\left(2 + ve^{i\phi} + ve^{-i\phi}\right) = \frac{1}{2}\left(1 + v\cos\phi\right)$$

as desired. [3 marks]
*New although a similar question was part of the problem sheet.*

(c) Vectors $|\,u_k\,\rangle$ form an orthonormal basis. Therefore the probability $P_0$ can be written as the sum:

$$\begin{aligned} P_0 &= \sum_k \frac{p_k}{4}\left(2 + \langle\,u_k\,|U|\,u_k\,\rangle + \langle\,u_k\,|U^{\dagger}|\,u_k\,\rangle\right) \\ &= \frac{1}{2} + \frac{1}{4}\left[\sum_k p_k\langle\,u_k\,|U|\,u_k\,\rangle + \sum_k \langle\,u_k\,|U^{\dagger}|\,u_k\,\rangle\right] \\ &= \frac{1}{2} + \frac{1}{4}\Bigg[\mathrm{Tr}\left(\sum_k p_k|\,u_k\,\rangle\langle\,u_k\,|\right)U + \mathrm{Tr}\left(\sum_k p_k|\,u_k\,\rangle\langle\,u_k\,|\right)U^{\dagger}\Bigg) \\ &= \frac{1}{2} + \frac{1}{4}\left[\mathrm{Tr}\,\rho U + \mathrm{Tr}\,\rho U^{\dagger}\right]. \end{aligned}$$

If we write

$$ve^{i\phi} = \mathrm{Tr}\,\rho U,$$

then $P_0$ becomes:

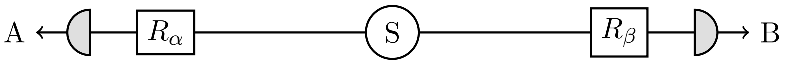
$$P_0 = \frac{1}{2}\left(1 + v\cos\phi\right) \qquad \text{[7 marks]}$$

*A variation of the question on the phase estimation from the problem sheet.*

(d) In order to estimate $\mathrm{Tr}\,\rho U$ we must be able to run the network many times with possibly another phase gate in between the Hadamard gates or alternatively allow for measurement in different bases. [1 mark]
The same network allows us to find an estimate for $\mathrm{Tr}\,U$ if we use $\rho = \frac{\mathbb{1}}{N}$ i.e the maximally mixed state and multiply the result by $N$. [2 marks]
*Covered in a class.*

2. (a) [4 marks] Two entangled qubits in state $\frac{1}{\sqrt{2}}(|\,00\,\rangle + |\,11\,\rangle)$ are generated by source $S$; one qubit is sent to Alice and one to Bob, who perform measurements in the computational basis. What is the probability that Alice and Bob will register identical results? Can any correlations they observe be used for instantaneous communication?

(b) [8 marks] Prior to the measurements in the computational basis Alice and Bob apply unitary operations $R_\alpha$ and $R_\beta$ to their respective qubits



The gate $R_\theta$ is defined by its action on the basis states

$$\begin{aligned} |\,0\,\rangle &\to \quad \cos\theta|\,0\,\rangle + \sin\theta|\,1\,\rangle,) \\ |\,1\,\rangle &\to -\sin\theta|\,0\,\rangle + \cos\theta|\,1\,\rangle. \end{aligned}$$

Show that the state of the two qubits prior to the measurements is

$$\cos(\alpha-\beta)\frac{1}{\sqrt{2}}\left(|\,00\,\rangle + |\,11\,\rangle\right) - \sin(\alpha-\beta)\frac{1}{\sqrt{2}}(|\,01\,\rangle - |\,10\,\rangle)$$

What is the probability that Alice and Bob's outcomes are identical?

(c) [5 marks] Let $A_1, A_2, B_1$ and $B_2$ be the measurements defined by the settings $\alpha_1 = 0$, $\alpha_2 = \frac{2\pi}{8}$, $\beta_1 = \frac{\pi}{8}$ and $\beta_2 = \frac{3\pi}{8}$, respectively. Alice and Bob perform a statistical test in which Alice repeatedly measures either $A_1$ or $A_2$ and Bob either $B_1$ or $B_2$. For each run they choose their settings randomly and independently from each other and check whether one of the following condition is satisfied

$$A_1 = B_1, \quad B_1 = A_2, \quad A_2 = B_2, \quad B_2 \neq A_1.$$

What is the probability (the fraction of the measurements) in which they find the outcomes in agreement with the four conditions?

(d) [4 marks] An adversary, Eve, who controls the source $S$, claims she has a way to predict outcomes $A_1, A_2, B_1$ and $B_2$ with certainty. Can such outcomes have pre-determined values?

(e) [4 marks] Explain how Alice and Bob, miles apart but able to communicate over a public channel, can use the scheme to establish a secret cryptographic key.

**Solution:**
*Most of this question was covered during the lectures and in the class, albeit using a different approach.*

(a) Alice and Bob will always obtain identical outcomes. [1 mark]
However, since the outcomes are random and cannot be enforced this does not allow Alice and Bob to communicate instantaneously. [3 marks]

(b) Applying the unitary operations $R_\alpha$ and $R_\beta$ to the entangled pair gives:

$$\begin{aligned}\frac{1}{\sqrt{2}}(|\,00\,\rangle + |\,11\,\rangle) \xrightarrow{R_\alpha \otimes R_\beta} \quad & \tfrac{1}{\sqrt{2}}[(\cos\alpha|\,0\,\rangle + \sin\alpha|\,1\,\rangle)(\cos\beta|\,0\,\rangle + \sin\beta|\,1\,\rangle) \\ & +(-\sin\alpha|\,0\,\rangle + \cos\alpha|\,1\,\rangle)(-\sin\beta|\,0\,\rangle + \cos\beta|\,1\,\rangle)]]\end{aligned}$$

Multiplying out the brackets:

$$\begin{aligned}&\tfrac{1}{\sqrt{2}}[(\cos\alpha\cos\beta + \sin\alpha\sin\beta)|\,0\,\rangle|\,0\,\rangle + (\sin\alpha\sin\beta + \cos\alpha\cos\beta)|\,1\,\rangle|\,1\,\rangle \\ &+(\cos\alpha\sin\beta - \sin\alpha\cos\beta)|\,0\,\rangle|\,1\,\rangle + (\sin\alpha\cos\beta - \cos\alpha\sin\beta)|\,1\,\rangle|\,0\,\rangle]\end{aligned}$$

and using standard trigonometric identities, we find :

$$\cos(\alpha-\beta)\frac{|\,00\,\rangle + |\,11\,\rangle}{\sqrt{2}} - \sin(\alpha-\beta)\frac{|\,01\,\rangle - |\,10\,\rangle}{\sqrt{2}}$$

The probability that Alice and Bob's outcomes are identical is just the square modulus of the corresponding amplitude i.e. $\cos^2(\alpha-\beta)$. [8 marks]

(c) The probabilities corresponding to each of the four conditions are:

$$\begin{aligned}P\,(A_1 = B_1) &= \cos^2(\alpha_1 - \beta_1) = \cos^2\left(\frac{\pi}{8}\right), \\ P\,(B_1 = A_2) &= \cos^2(\beta_1 - \alpha_2) = \cos^2\left(\frac{\pi}{8}\right), \\ P\,(A_2 = B_2) &= \cos^2(\alpha_2 - \beta_2) = \cos^2\left(\frac{\pi}{8}\right), \\ P\,(B_2 \neq A_1) &= \sin^2(\beta_2 - \alpha_1) = \sin^2\left(\frac{3\pi}{8}\right) = \cos^2\left(\frac{\pi}{8}\right).\end{aligned}$$

Regardless which setting they choose they find the outcomes satisying the conditions with probability $\cos^2\left(\frac{\pi}{8}\right) \approx 0.85$ [5 marks]

(d) With pre-determined values at least one of the four conditions would not be satisfied and the highest achievable probability would be $\frac{3}{4} = 0.8 = 75$. Hence the values cannot be pre-determined. [4 marks]

(e) The above scheme can be used to establish the following key distribution protocol:

1. Initially, a large number of Bell pairs is generated by source S and sent to Alice and Bob who repeatedly perform their measurements, with the measurements settings chosen randomly and independently between $A_1$ and $A_2$ by Alice nad $B_1$ and $B_2$ by Bob.
2. Alice and Bob share the choices of their measurement setting for each run via the public channel.
3. Next they choose a random subset of their measurements and reveal the corresponding outcomes to estimate the probability in which the results are in agreement with the four conditions. If the probability is smaller than 0.75 then they start the protocol from scratch. Otherwise, they can use the remaining results as the key. If the probability is in the 0.75 to 0.85 range, then they have to employ privacy amplification methods to distill a perfect key. [4 marks]

3. The controlled-not is a two-qubit gate defined in the computational basis as

$$|\,x\,\rangle|\,y\,\rangle \mapsto |\,x\,\rangle|\,x \oplus y\,\rangle,$$

where $x, y = 0, 1$.

(a) [4 marks] If the second qubit is prepared in state $|\,0\,\rangle$ ($y = 0$) the gate clones the bit value of the first qubit $|\,x\,\rangle|\,0\,\rangle \mapsto |\,x\,\rangle|\,x\,\rangle$. Show that this does not imply that $|\,\psi\,\rangle|\,0\,\rangle \mapsto |\,\psi\,\rangle|\,\psi\,\rangle$ for any quantum state $|\,\psi\,\rangle$ of the first qubit.

(b) [6 marks] A universal quantum cloner is a hypothetical quantum device that operates on two qubits and on some auxiliary system. Given one qubit in any quantum state $|\,\psi\,\rangle$ and the other one in a prescribed state $|\,0\,\rangle$ it maps

$$|\,\psi\,\rangle|\,0\,\rangle|\,R\,\rangle \mapsto |\,\psi\,\rangle|\,\psi\,\rangle|\,R'\,\rangle,$$

where $|\,R\,\rangle$ and $|\,R'\,\rangle$ are, respectively, the initial and the final state of any other auxiliary system that may participate in the cloning process ($|\,R'\,\rangle$ may depend on $|\,\psi\,\rangle$). Show that such a cloner is impossible.

(c) [3 marks] The best approximation to the universal quantum cloner is the following transformation

$$|\,\psi\,\rangle|\,0\,\rangle|\,0\,\rangle \mapsto \sqrt{\frac{2}{3}}|\,\psi\,\rangle|\,\psi\,\rangle|\,\psi\,\rangle + \sqrt{\frac{1}{6}}\Big(|\,\psi\,\rangle|\,\psi^{\perp}\,\rangle + |\,\psi^{\perp}\,\rangle|\,\psi\,\rangle\Big)|\,\psi^{\perp}\,\rangle$$

where $|\,\psi^{\perp}\,\rangle$ is a normalised state vector orthogonal to $|\,\psi\,\rangle$ and the auxiliary system is another qubit. Explain why the reduced density matrices of the first and the second qubit must be identical.

(d) [9 marks] Show that the reduced density matrix of the first (and the second) qubit can be written as

$$\rho = \frac{5}{6}|\,\psi\,\rangle\langle\,\psi\,| + \frac{1}{6}|\,\psi^{\perp}\,\rangle\langle\,\psi^{\perp}\,|.$$

(e) [3 marks] What is the probability that the clone in state $\rho$ will pass a test for being the original in state $|\,\psi\,\rangle$?

**Solution:**

(a) Consider a general qubit state:

$$|\,\psi\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle.$$

The controlled-not transforms this state into:

$$(\alpha|\,0\,\rangle + \beta|\,1\,\rangle)\,|\,0\,\rangle \mapsto \alpha|\,0\,\rangle|\,0\,\rangle + \beta|\,1\,\rangle|\,1\,\rangle,$$

which is different from

$$|\,\psi\,\rangle|\,\psi\,\rangle = \alpha^2|\,0\,\rangle|\,0\,\rangle + \alpha\beta\,(|\,0\,\rangle|\,1\,\rangle + |\,1\,\rangle|\,0\,\rangle) + \beta^2|\,1\,\rangle|\,1\,\rangle$$

for arbitrary $\alpha$ and $\beta$. [4 marks]
*Covered in the lectures.*

(b) Take $|\,a\,\rangle$ and $|\,b\,\rangle$ to be two arbitrary pure quantum states. The universal quantum cloner device would map:

$$\begin{aligned} |\,a\,\rangle|\,0\,\rangle|\,R\,\rangle &\mapsto |\,a\,\rangle|\,a\,\rangle|\,R'\,\rangle \\ |\,b\,\rangle|\,0\,\rangle|\,R\,\rangle &\mapsto |\,b\,\rangle|\,b\,\rangle|\,R''\,\rangle. \qquad \text{[2 marks]} \end{aligned}$$

Quantum evolutions are unitary and therefore they preserve inner products. Taking the scalar product between the two equations above we find:

$$\langle a|b\rangle = \langle a|b\rangle^2 \langle R'|R''\rangle.$$

The modulus of each of the scalar products is $\leqslant 1$ which implies that we either need to have $\langle a|b\rangle = 0$ or $\langle a|b\rangle = 1$ and $\langle R'|R''\rangle = 1$, meaning that the two states $|\,a\,\rangle$ and $|\,b\,\rangle$ are either orthogonal or equal to each other. This is in contradiction with our assumption that $|\,a\,\rangle$ and $|\,b\,\rangle$ are arbitrary. Therefore, there does not exists a quantum device that could clone any quantum state $|\,\psi\,\rangle$. [4 marks]

*A standard proof the no-cloning theorem that was covered in the lectures. The rest of the problem is new.*

(c) The state

$$\sqrt{\frac{2}{3}}|\,\psi\,\rangle|\,\psi\,\rangle|\,\psi\,\rangle + \sqrt{\frac{1}{6}}\left(|\,\psi\,\rangle|\,\psi^{\perp}\,\rangle + |\,\psi^{\perp}\,\rangle|\,\psi\,\rangle\right)|\,\psi^{\perp}\,\rangle$$

is invariant under the exchange of 1st qubit with 2nd qubit. Hence the reduced density matrices must be the same. [3 marks]

(d) Notice that we can rewrite the state of three qubits as:

$$|\,\psi\,\rangle\left(\sqrt{\frac{2}{3}}|\,\psi\,\rangle|\,\psi\,\rangle + \sqrt{\frac{1}{6}}|\,\psi^{\perp}\,\rangle|\,\psi^{\perp}\,\rangle\right) + |\,\psi^{\perp}\,\rangle\left(\sqrt{\frac{1}{6}}|\,\psi\,\rangle|\,\psi^{\perp}\,\rangle\right).$$

The two-qubit states in the brackets are orthogonal to each other. Therefore taking the partial trace over those two qubits gives:

$$\rho = |\,\psi\,\rangle\langle\,\psi\,|\left(\frac{2}{3}+\frac{1}{6}\right) + |\,\psi^{\perp}\,\rangle\langle\,\psi^{\perp}\,|\left(\frac{1}{6}\right) = \frac{5}{6}|\,\psi\,\rangle\langle\,\psi\,| + \frac{1}{6}|\,\psi^{\perp}\,\rangle\langle\,\psi^{\perp}\,|. \qquad \text{[9 marks]}$$

(e) The probability that the clone in state $\rho$ will pass a test for being in the original $|\,\psi\,\rangle$ is given by the standard formula:

$$p_{\psi} = \mathrm{Tr}\,(|\,\psi\,\rangle\langle\,\psi\,|\rho) = \langle\,\psi\,|\rho|\,\psi\,\rangle = \frac{5}{6}. \qquad \text{[3 marks]}$$