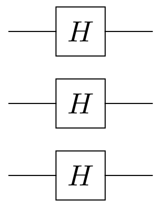
C7.4 Introduction to Quantum Information

Model Solutions

1. (a) [3 marks] *[Classification: B]* The Hadamard transform is often useful as the first operation in quantum algorithms because, when applied to n bits, it prepares an equally weighted superposition of all the numbers 0 to $2^n - 1$, so that all these numbers can be tested simultaneously. Its quantum network should consist of a series of n wires with the single-qubit Hadamard gate H applied to each of them:



(b) [4 marks] *[Classification: B]* The first two computational steps end up with the quantum function evaluation and generate the state

$$|\,0\,\rangle|\,0\,\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,0\,\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,f(x)\,\rangle.$$

This is an entangled state of the two registers. Here and in the following $|\,0\,\rangle$ represents a binary string of length n with all qubits showing logical 0.

(c) [5 marks] *[Classification: S]* If $k \in \{0,1\}^n$ is the result of the bit-by-bit measurement on the second register then the state of the first register is a superposition of exactly those values of x for which $f(x) = k$. We can write it as

$$\frac{1}{\sqrt{2}} \left(|\,x\,\rangle + |\,x+s\,\rangle\right).$$

for some x, such that $f(x) = f(x+s) = k$.

(d) [6 marks] *[Classification: S]* The Hadamard transform applied to the first register after the function evaluation and the measurement on the second register gives

$$\begin{aligned}\frac{1}{\sqrt{2}} \left(|\,x\,\rangle + |\,x+s\,\rangle\right) \mapsto & \frac{1}{\sqrt{2^{n+1}}} \sum_{z\in\{0,1\}^n} \left[(-1)^{x\cdot z} + (-1)^{(x+s)\cdot z}\right] |\,z\,\rangle \\ = & \frac{1}{\sqrt{2^{n+1}}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} \left[1 + (-1)^{s\cdot z}\right] |\,z\,\rangle.\end{aligned}$$

When the first register is subsequently measured bit-by-bit in the computational basis, the probability of getting a particular binary string z is

$$\frac{1}{2^{n+1}} \left(1 + (-1)^{s\cdot z}\right)^2 = \begin{cases} 1/2^{n-1} & , \quad \text{if } s\cdot z = 0 \\ 0 & , \quad \text{if } s\cdot z = 1 \end{cases}$$

(e) [7 marks] *[Classification: N]* Students should be able to provide estimates and plausibility arguments. More detailed explanations, as presented below, are not required.

Students should notice that running the quantum network gives us a method for extracting uniformly random strings z such that $s \cdot z = 0$ for our unknown s. If $z \neq 0$, then this cuts in half the number of possible s strings consistent with this equation. In order to find s we need $n-1$ such equations, $z_1 \cdot s = 0, z_2 \cdot s = 0, \ldots z_{n-1} \cdot s = 0$, with the z_i being linearly independent ($s = 0$ is always a solution but we have excluded it). The probability of obtaining $n-1$ independent binary strings of length n via random sampling can be estimated in many ways. For example, one can notice that m linearly independent vectors $z_1, z_2, \ldots z_m$, specify a subspace with 2^m bit strings. The probability that the next bit string z_{m+1} is linearly independent is $(2^n - 2^m)/2^n$. Chaining these conditional probabilities we obtain the probability of getting $n-1$ linearly independent bit strings,

$$\Pr = \left(1 - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^{n-1}}\right)\cdots\left(1 - \frac{1}{4}\right).$$

To bound this we then use the fact that $(1-a)(1-b) \geqslant 1 - a - b$ for $0 \leqslant a, b \leqslant 1$ to turn the products into a sum,

$$\Pr \geqslant 1 - \left(\frac{1}{2^n} + \frac{1}{2^{n-1}} + \cdots + \frac{1}{4}\right) > \frac{1}{2}.$$

Thus with probability of greater than $1/2$ we obtain $n-1$ linearly independent bit strings z_i and can solve for s. We may need to repeat this process a few times; the probability that we fail to find s decreases exponentially with the number of repetitions. Thus the number of runs for the quantum algorithm is of the order of n.

In contrast a classical algorithm randomly chooses $x_1, x_2, \ldots x_k$, evaluates $f(x_1), f(x_2)$, $\ldots f(x_k)$ and checks for collision events where $f(x_i) = f(x_j)$ for some x_i and x_j ($s = x_i + x_j$). The probability for at least one collision can be estimated in a number of different ways (the birthday paradox type calculations) and it is not greater than $k^2/2^n$. This implies that we have to sample roughly $\sqrt{2^n}$ times in order to find a collision (and hence s).

2. (a) [2 marks] *[Classification: B]* The diagonal elements of a density matrix (in any basis) are interpreted as probabilities. They are nonnegative and add up to one.

   (b) [7 marks] *[Classification: B and S]* Students should write

$$\psi = \frac{1}{\sqrt{3}}|\,0,0\,\rangle - \frac{1}{\sqrt{6}}|\,0,1\,\rangle + \frac{1}{\sqrt{3}}|\,1,0\,\rangle + \frac{1}{\sqrt{6}}|\,1,1\,\rangle$$

and $\rho = |\,\psi\,\rangle\langle\,\psi\,|$. This gives

$$\begin{aligned}
\rho =& \frac{1}{3}|\,0,0\,\rangle\langle\,0,0\,| - \frac{1}{3\sqrt{2}}|\,0,0\,\rangle\langle\,0,1\,| + \frac{1}{3}|\,0,0\,\rangle\langle\,1,0\,| + \frac{1}{3\sqrt{2}}|\,0,0\,\rangle\langle\,1,1\,| \\
&- \frac{1}{3\sqrt{2}}|\,0,1\,\rangle\langle\,0,0\,| + \frac{1}{6}|\,0,1\,\rangle\langle\,0,1\,| - \frac{1}{3\sqrt{2}}|\,0,1\,\rangle\langle\,1,0\,| - \frac{1}{6}|\,0,1\,\rangle\langle\,1,1\,| \\
&+ \frac{1}{3}|\,1,0\,\rangle\langle\,0,0\,| - \frac{1}{3\sqrt{2}}|\,1,0\,\rangle\langle\,0,1\,| + \frac{1}{3}|\,1,0\,\rangle\langle\,1,0\,| + \frac{1}{3\sqrt{2}}|\,1,0\,\rangle\langle\,1,1\,| \\
&+ \frac{1}{3\sqrt{2}}|\,1,1\,\rangle\langle\,0,0\,| - \frac{1}{6}|\,1,1\,\rangle\langle\,0,1\,| + \frac{1}{3\sqrt{2}}|\,1,1\,\rangle\langle\,1,0\,| + \frac{1}{6}|\,1,1\,\rangle\langle\,1,1\,|.
\end{aligned}$$

In the $\{|\,00\,\rangle, |\,01\,\rangle, |\,10\,\rangle, |\,11\,\rangle\}$ basis, the matrix representation of ρ is

$$\rho = \frac{1}{3}\begin{pmatrix} 1 & -\frac{1}{\sqrt{2}} & 1 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{2} & -\frac{1}{\sqrt{2}} & -\frac{1}{2} \\ 1 & -\frac{1}{\sqrt{2}} & 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \end{pmatrix}.$$

(c) [4 marks] *[Classification: B and S]* The reduced density operator ρ_1 of qubit 1 is

$$\rho_1 = \mathrm{Tr}_2\, \rho = \frac{1}{2}\begin{pmatrix} 1 & \frac{1}{3} \\ \frac{1}{3} & 1 \end{pmatrix}. \tag{1}$$

Likewise, the reduced density matrix $\rho_2 = \mathrm{Tr}_1\, \rho$ is

$$\rho_2 = \mathrm{Tr}_1\, \rho = \frac{1}{3}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

(d) [5 marks] *[Classification: easy N]* For any self-adjoint matrix A we can find an orthonormal basis such that A is diagonal, and the diagonal elements are its eigenvalues λ_i,

$$A = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_n \end{pmatrix}.$$

Choosing the eigenbasis of A when evaluating the trace, we get

$$\mathrm{Tr}\left(\sqrt{A^\dagger A}\right) = \sum_{i=1}^{n} \sqrt{\lambda_i^2} = \sum_{i=1}^{n} |\lambda_i|.$$

Since all eigenvalues of a density matrix are non-negative and add up to unity, the trace norm of of a density matrix is equal to one.

(e) [7 marks] *[Classification: N]* We need to calculate the trace distance between the reduced density matrices in (c). We have

$$\rho_1 - \rho_2 = \frac{1}{6}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad (\rho_1 - \rho_2)^\dagger(\rho_1 - \rho_2) = \frac{1}{18}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2}$$

This gives

$$||\rho_1 - \rho_2||_{tr} = \frac{2}{3\sqrt{2}} \quad \text{and} \quad T(\rho_1, \rho_2) = \frac{1}{3\sqrt{2}}.$$

The maximal probability $P_{\max}$ with which we can distinguish the two qubits in a single measurement is thus

$$P_{\max} = \frac{1}{2}\left(1 + \frac{1}{3\sqrt{2}}\right) = \frac{1}{12}(6 + \sqrt{2}) \approx 0.62.$$

3. (a) [6 marks] *[Classification: B]* The single-qubit Hadamard gate is given by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The interference network effects the following sequence of transformations,

$$\begin{aligned}
|\,0\,\rangle &\overset{H}{\mapsto} \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle) \\
&\overset{\varphi}{\mapsto} \frac{1}{\sqrt{2}}(|\,0\,\rangle + e^{i\varphi}|\,1\,\rangle) \\
&\overset{H}{\mapsto} \frac{1}{2}\left[|\,0\,\rangle + |\,1\,\rangle + e^{i\varphi}(|\,0\,\rangle - |\,1\,\rangle)\right] \\
&= \frac{1}{2}e^{i\varphi/2}\left[\left(e^{i\varphi/2} + e^{-i\varphi/2}\right)|\,0\,\rangle - \left(e^{i\varphi/2} - e^{-i\varphi/2}\right)|\,1\,\rangle\right] \\
&= e^{i\varphi/2}\left[\cos\frac{\varphi}{2}|\,0\,\rangle - i\sin\frac{\varphi}{2}|\,1\,\rangle\right].
\end{aligned}$$

The output state is thus given by

$$| \psi_{\text{out}} \rangle = e^{i\varphi/2} \left[\cos \frac{\varphi}{2} | 0 \rangle - i \sin \frac{\varphi}{2} | 1 \rangle \right].$$

The probability for the qubit to be in state $| 0 \rangle$ at the output is

$$P_0 = |\langle 0 | \psi_{\text{out}} \rangle|^2 = \cos^2 \frac{\varphi}{2}.$$

(b) [12 marks] *[Classification: S]* If we follow the same steps as in (a) including the environment and the decoherence process we find

$$\begin{aligned} | 0 \rangle | e \rangle &\overset{H}{\mapsto} \frac{1}{\sqrt{2}} (| 0 \rangle + | 1 \rangle) | e \rangle \\ &\overset{\varphi}{\mapsto} \frac{1}{\sqrt{2}} (| 0 \rangle + e^{i\varphi} | 1 \rangle) | e \rangle \\ &\overset{\text{dec.}}{\mapsto} \frac{1}{\sqrt{2}} \left[| 0 \rangle | e_0 \rangle + e^{i\varphi} | 1 \rangle | e_1 \rangle \right] \\ &\overset{H}{\mapsto} \frac{1}{2} \left[(| 0 \rangle + | 1 \rangle) | e_0 \rangle + e^{i\varphi} (| 0 \rangle - | 1 \rangle) | e_1 \rangle \right]. \end{aligned}$$

The output state, including the environment, can thus be written as

$$| \psi_{\text{out}} \rangle = \frac{1}{2} \left[| 0 \rangle \left(| e_0 \rangle + e^{i\varphi} | e_1 \rangle \right) + | 1 \rangle \left(| e_0 \rangle - e^{i\varphi} | e_1 \rangle \right) \right].$$

[4 marks up to here.]
The probability for the qubit to be in state $| 0 \rangle$ at the output is now

$$\begin{aligned} P_0 &= \text{Tr} \left[(| \psi_{\text{out}} \rangle \langle \psi_{\text{out}} |)(| 0 \rangle \langle 0 | \otimes \mathbb{1}_{\text{E}}) \right], \\ &= \frac{1}{4} \text{Tr}_{\text{E}} \left[\left(| e_0 \rangle + e^{i\varphi} | e_1 \rangle \right) \left(\langle e_0 | + e^{-i\varphi} \langle e_1 | \right) \right], \\ &= \frac{1}{4} \left(\langle e_0 | e_0 \rangle + \langle e_1 | e_1 \rangle + e^{i\varphi} \langle e_0 | e_1 \rangle + e^{-i\varphi} \langle e_1 | e_0 \rangle \right], \end{aligned}$$

where Tr denotes the trace over the qubit and the environment, Tr_{E} is the trace over the environment and $\mathbb{1}_{\text{E}}$ is the identity operator acting on the state space of the environment. *[4 marks for the correct expression for P_0.]*
If we write $\langle e_0 | e_1 \rangle = v e^{i\alpha}$ and use $\langle e_0 | e_0 \rangle = \langle e_1 | e_1 \rangle = 1$, then we find

$$P_0(\varphi, v, \alpha) = \frac{1}{4} \left[2 + v \left(e^{i(\varphi+\alpha)} + e^{-i(\varphi+\alpha)} \right) \right] = \frac{1}{2} \left[1 + v \cos(\varphi + \alpha) \right].$$

[2 marks for the correct final answer.]
If the decoherence takes place between the first Hadamard gate and the phase gate, the expression for $P_0(\varphi, v, \alpha)$ remains the same. *[2 marks]*

(c) [7 marks] *[Classification: N]* As $v = |\langle e_0 | e_1 \rangle|$ decreases, we lose all the advantages of quantum interference. In Deutsch's algorithm we have effectively $\varphi = 0$ if f is constant or $\varphi = \pi$ if f is balanced. Thus we obtain the correct answer with probability at most $(1 + v)/2$. For $\langle e_0 | e_1 \rangle = 0$, the perfect decoherence case, the network outputs 0 or 1 with equal probabilities, *i.e.* it is useless as a computing device. It is clear that we want to avoid decoherence, or at least diminish its impact on our computing device.