Final Honour School of Mathematics Part C

C7.4 Introduction to Quantum Information
Artur Ekert
Checked by: Lionel Mason

April 30, 2020

ABD: EveryShipout initializing macros

Do not turn this page until you are told that you may do so

1. The Hadamard transform on n qubits is defined as

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

where $x, y \in \{0,1\}^n$ and $x \cdot y \equiv (x_1 \cdot y_1) \oplus \ldots \oplus (x_n \cdot y_n)$.

(a) [3 marks] Sketch the quantum circuit which effects the Hadamard transform and explain why it is useful as the first operation in quantum algorithms.

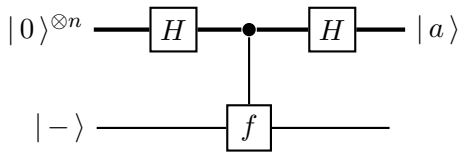
You are presented with an oracle that computes some unknown function $f\colon \{0,1\}^n \to \{0,1\}$, but you are promised that f is of the form

$$f(x) = a \cdot x \equiv (a_1 \cdot x_1) \oplus \ldots \oplus (a_n \cdot x_n),$$

for some fixed $a \in \{0,1\}^n$. Your task is to determine the value of the n-bit string a using the fewest queries possible.

(b) [3 marks] How many calls to the oracle are required to determine a if the oracle is classical?

(c) [7 marks] The circuit below implements a quantum algorithm which outputs the value of a with a single call to the (quantum) oracle. In the diagram the H operations in the first register denote the Hadamard transform on n qubits and the f operation represents the oracle, i.e., a quantum evaluation of $f\colon |\,x\,\rangle|\,y\,\rangle \mapsto |\,x\,\rangle|\,y \oplus f(x)\,\rangle$. The second register, to which the value $f(x)$ is added, contains one qubit prepared in state $|-\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle - |\,1\,\rangle)$.



Step through the execution of this circuit, writing down quantum states of the two registers after each computational step. Explain how the value of a is obtained.

(d) [5 marks] If the state of the second register, $|-\rangle$, is replaced with $|+\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle)$, prove that you learn nothing about the value of a by running this circuit.

(e) [7 marks] The network construction presented here can be generalised to the case of a Boolean function $f : \{0,1\}^n \mapsto \{0,1\}^m$. Suppose the second register contains m qubits and the oracle evaluates the function $f(x) = A \cdot x$ (modulo 2) where A is an $m \times n$ binary matrix. By running the network m times with suitable choices for the states of the second register all the entries of A can be determined. Explain how.

2. Any density matrix of a single qubit can be parameterised by the three real components of the Bloch vector $\vec{s} = (s_x, s_y, s_z)$ and written as

$$\varrho = \tfrac{1}{2}\left(\mathbb{1} + \vec{s}\cdot\vec{\sigma}\right),$$

where σ_x, σ_y and σ_z are the Pauli matrices, and $\vec{s}\cdot\vec{\sigma} = s_x\sigma_x + s_y\sigma_y + s_z\sigma_z$.

(a) [2 marks] Express the eigenvalues of ϱ in terms of the length of $\vec{s}$ and explain why the length of the Bloch vector cannot exceed 1.

(b) [3 marks] Show that for any two density operators ϱ_1 and ϱ_2, $\mathrm{Tr}(\varrho_1\varrho_2) = \frac{1}{2}(1 + \vec{s}_1\cdot\vec{s}_2)$, where $\vec{s}_1$ and $\vec{s}_2$ are the Bloch vectors of ϱ_1 and ϱ_2, respectively.

(c) [3 marks] Show that unitary evolutions, $\varrho \mapsto U\varrho U^\dagger$ preserve the scalar product of Bloch vectors and deduce that such evolutions correspond to rotations of the Bloch sphere. Describe these rotations for the Pauli unitaries σ_x, σ_y and σ_z.

(d) [3 marks] A qubit in state ϱ is transmitted through a depolarising channel that effects a completely positive map

$$\varrho \mapsto (1-p)\varrho + \frac{p}{3}\left(\sigma_x\varrho\sigma_x + \sigma_y\varrho\sigma_y + \sigma_z\varrho\sigma_z\right),$$

for some $0 \leqslant p \leqslant 1$. Show that under this map the Bloch vector associated with ϱ shrinks by the factor $(3-4p)/3$.

The trace norm of a matrix A is defined as

$$|A|_{\mathrm{tr}} = \mathrm{Tr}\left(\sqrt{A^\dagger A}\right).$$

(e) [2 marks] Explain why the trace norm of any self-adjoint matrix is the sum of the absolute values of its eigenvalues. What is the trace norm of a density matrix?

If a physical system is equally likely to be prepared either in state ϱ_1 or state ϱ_2 then a single measurement can distinguish between the two preparations with the probability at most

$$P_S = \frac{1}{2} + \frac{1}{4}\left|\varrho_1 - \varrho_2\right|_{\mathrm{tr}}, \tag{1}$$

where $\frac{1}{2}\left|\varrho_1 - \varrho_2\right|_{\mathrm{tr}}$ is known as the trace distance between ϱ_1 and ϱ_2.

(f) [4 marks] Explain why the statement above implies that all physically admissible operations can only reduce the trace distance between density operators.

(g) [4 marks] A qubit is equally likely to be prepared either in state ϱ_1 or state ϱ_2. Show that

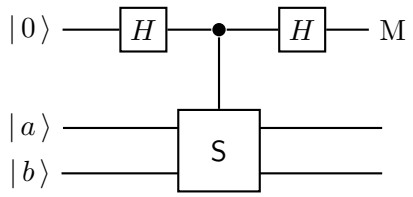
$$P_S = \frac{1}{2} + \frac{1}{4}\left|\vec{s}_1 - \vec{s}_2\right|.$$

(h) [4 marks] Show that unitary evolutions do not degrade distinguishability of quantum states but the depolarising channel does. By how much is P_S decreased by the action of the depolarising channel?

3. The swap gate S on two qubits is defined first on product vectors, $S : |\,a\,\rangle \otimes |\,b\,\rangle \mapsto |\,b\,\rangle \otimes |\,a\,\rangle$ and then extended to sums of product vectors by linearity.

   (a) [3 marks] Show that $P_\pm = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors which form the decomposition of the identity and project on the symmetric and the antisymmetric subspaces. Decompose the state vector $|\,a\,\rangle|\,b\,\rangle$ of two qubits into symmetric and antisymmetric components.

Consider the following "swap-test" quantum circuit composed of two Hadamard gates, one controlled-S operation and the measurement M in the computational basis,



The state vectors $|\,a\,\rangle$ and $|\,b\,\rangle$ of the target qubits are normalised but not orthogonal to each other.

   (b) [5 marks] Step through the execution of this circuit, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed? Explain why this circuit implements projections on the symmetric and the antisymmetric subspaces of the two target qubits.

   (c) [3 marks] Does the measurement result $M = 0$ imply that $|\,a\,\rangle$ and $|\,b\,\rangle$ are identical? Does the measurement result $M = 1$ imply that $|\,a\,\rangle$ and $|\,b\,\rangle$ are not identical?

   (d) [5 marks] Suppose an efficient quantum algorithm encodes information about a complicated graph into a pure state of a qubit. Graphs which are isomorphic are mapped into the same state of the qubit. Given two complicated graphs your task is to check if they are isomorphic. You can run the algorithm as many times as you want and you can use the "swap-test" circuit. How would you accomplish this task?

   (e) [6 marks] Instead of the state $|\,a\,\rangle \otimes |\,b\,\rangle$ the two target qubits are prepared in some mixed state $\rho_a \otimes \rho_b$. Show that the probability of successful projection of this state on the symmetric subspace is

$$\frac{1}{2}\left(1 + \mathrm{Tr}\,\rho_a\rho_b\right).$$

   (f) [3 marks] Does the measurement result $M = 1$ imply that ρ_a and ρ_b are not identical?

[*In the computational basis, the Pauli matrices σ_x, σ_y, and σ_z are*

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

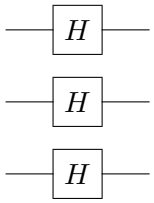
They anticommute and square to the identity: $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}$. They also satisfy:

$$(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = (\vec{a}\cdot\vec{b})\,\mathbb{1} + i(\vec{a}\times\vec{b})\cdot\vec{\sigma},$$

for any two Euclidean vectors $\vec{a}$ and $\vec{b}$.]

SOLUTIONS: QUESTION 1

1. (a) [3 marks] [BOOKWORK] The Hadamard transform is often useful as the first operation in quantum algorithms because, when applied to n qubits, it prepares an equally weighted superposition of all the binary string $x \in \{0,1\}^n$, so that all these strings can be tested simultaneously. Its quantum circuit should consist a series of n wires with the gate H applied to each of them:



(b) [3 marks] [BOOKWORK] If we input a value $x = 00\ldots010\ldots0$, with the 1 on bit m, then $f(x)$ is simply the m^{th} bit of a. After n similar calls, we can evaluate every bit value. It is also clear that there cannot exist a better classical algorithm – each call to the oracle teaches us exactly one bit of information, and since we must learn n bits, we must query it n times.

(c) [7 marks] [BOOKWORK / SIMILAR] The first step is a typical opening for most of quantum algorithms

$$|\,0\,\rangle|\,-\,\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,-\,\rangle$$

The function evaluation gives

$$\begin{aligned} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,-\,\rangle &\mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle(|\,0\oplus f(x)\,\rangle - |\,1\oplus f(x)\,\rangle)/\sqrt{2} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|\,x\,\rangle|\,-\,\rangle \end{aligned}$$

The state of the second register remains unchanged. The first register is further modified by the Hadamard transform

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|\,x\,\rangle \mapsto \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} (-1)^{(a\oplus z)\cdot x}|\,z\,\rangle = |\,a\,\rangle.$$

This is because $\sum_x (-1)^{(a\oplus z)\cdot x} = 0$ for all $a \oplus z$ apart from $a \oplus z = 0^{\otimes n}$. The final state of the two registers is $|\,a\,\rangle|\,-\,\rangle$. The bit by bit measurement of the first register gives a.

(d) [5 marks] [NEW] This follows the same reasoning as the previous step. The function evaluation gives

$$\begin{aligned} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,+\,\rangle &\mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle(|\,0\oplus f(x)\,\rangle + |\,1\oplus f(x)\,\rangle/\sqrt{2} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\,\rangle|\,+\,\rangle \end{aligned}$$

so that when we apply the final Hadamard transform, we get $|\,0\,\rangle^{\otimes n}|\,+\,\rangle$. Hence, there is no information about a in the state.

(e) [7 marks] [NEW] One should think of the k^{th} row of A as a bit string $a_k \in \{0,1\}^n$, and so we are effectively performing the original algorithm m times in parallel (once for each row, on a different qubit for the second register). The 'phase kick-back' is additive between these cases. From the previous part, we know how to get no phase kick-back in a given evaluation; just use the state $|+\rangle$ on the second register.

If $m-1$ qubits in the second register are prepared in state $|+\rangle$ and one qubit, say the kth qubit, is prepared in state $|-\rangle$ then the output of the first register will be the kth row of A. Repeat this for each value of $k = 1 \ldots m$.

SOLUTIONS: QUESTION 2

(a) [2 marks] [BOOKWORK] The two eigenvalues of

$$\rho = \frac{1}{2}\begin{bmatrix} 1+s_z & s_x - i\,s_y \\ s_x + i\,s_y & 1-s_z \end{bmatrix}$$

are $\frac{1}{2}(1 \pm \sqrt{s_x^2+s_y^2+s_z^2}) = \frac{1}{2}(1 \pm |\vec{s}|)$ hence, for $\rho \geqslant 0$ we must require that $|\vec{s}| \leqslant 1$.

(b) [3 marks] [SIMILAR] Pauli matrices are traceless, hence

$$\mathrm{Tr}(\rho_1\rho_2) = \mathrm{Tr}\left[\frac{1}{2}(\mathbb{1}+\vec{s}_1\cdot\vec{\sigma}_1)\frac{1}{2}(\mathbb{1}+\vec{s}_2\cdot\vec{\sigma}_2)\right] = \frac{1}{4}\left\{\mathrm{Tr}\,\mathbb{1} + \mathrm{Tr}\left[(\vec{s}_1\cdot\vec{s}_2)\,\mathbb{1}\right]\right\} = \frac{1}{2}(1+\vec{s}_1\cdot\vec{s}_2).$$

(c) [3 marks] [NEW] We use the cyclic properties of the trace,

$$\mathrm{Tr}\Big(U\rho_1U^\dagger U\rho_2U^\dagger\Big) = \mathrm{Tr}(\rho_1\rho_2) \implies \vec{s}_1\cdot\vec{s}_2 = \text{const.}$$

The only isometries of the Bloch sphere that preserve the scalar product and connect to the identity are rotations.

$$\begin{aligned}
\sigma_x\frac{1}{2}(\mathbb{1}+s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\sigma_x &= \frac{1}{2}(\mathbb{1}+s_x\sigma_x-s_y\sigma_y-s_z\sigma_z)\\
\sigma_y\frac{1}{2}(\mathbb{1}+s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\sigma_y &= \frac{1}{2}(\mathbb{1}-s_x\sigma_x+s_y\sigma_y-s_z\sigma_z)\\
\sigma_z\frac{1}{2}(\mathbb{1}+s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\sigma_z &= \frac{1}{2}(\mathbb{1}-s_x\sigma_x-s_y\sigma_y+s_z\sigma_z)
\end{aligned}$$

The Pauli unitaries σ_x, σ_y and σ_z rotate the Bloch vector by 180° around the x, y and z axes respectively.

(d) [3 marks] [SIMILAR] The modified Bloch vector is the sum of two parts. The original Bloch vector multiplied by factor $1-p$ (the first term in the definition of the depolarising channel) and the flipped Bloch vector (the combined action of σ_x, σ_y and σ_z) multiplied by factor $p/3$. Hence the Bloch vector shrinks by the factor $(1-p-p/3) = 1-4p/3$.

(e) [2 marks] [BOOKWORK]Use the diagonal representation of A and the definition of the norm. The trace norm of any density operator is 1.

(f) [4 marks] [NEW] A physically admissible map that could increase the trace distance would also increase P_S, in contradiction with the statement that P_S is the largest possible probability.

(g) [4 marks] [NEW]

$$\rho_1-\rho_2 = \frac{1}{2}(\vec{s}_1-\vec{s}_2)\cdot\vec{\sigma} \implies \mathrm{Tr}\sqrt{(\rho_1-\rho_2)^2} = \frac{1}{2}\,\mathrm{Tr}\sqrt{|\vec{s}_1-\vec{s}_2|^2\,\mathbb{1}} = |\vec{s}_1-\vec{s}_2|$$

(h) [4 marks] [NEW] Unitary evolutions are represented by rotations of the Bloch sphere which preserve $|\vec{s}_1-\vec{s}_2|$. The depolarising channel will reduce $|\vec{s}_1-\vec{s}_2|$ by a factor $(1-4p/3)$. Hence, after the depolarising channel P_S will be decreased by $-(4p/3)|\vec{s}_1-\vec{s}_2|$.

SOLUTIONS: QUESTION 3

(a) [3 marks] [New but based on standard material] Using $S^2 = \mathbb{1}$, we get: $P_+P_- = 0$ and $P_\pm^2 = P_\pm$, which confirms that $P_\pm$ are orthogonal projectors. Applying them to $|\,a\,\rangle|\,b\,\rangle$:

$$\begin{aligned} P_+(|\,a\,\rangle|\,b\,\rangle) &= \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle) + |\,b\,\rangle|\,a\,\rangle) \\ P_-(|\,a\,\rangle|\,b\,\rangle) &= \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle) - |\,b\,\rangle|\,a\,\rangle). \end{aligned}$$

(b) [5 marks] [SIMILAR] Stepping through the circuit

$$\begin{aligned} |\,0\,\rangle|\,a\,\rangle|\,b\,\rangle &\mapsto \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle)|\,a\,\rangle|\,b\,\rangle && (2) \\ &\mapsto \frac{1}{\sqrt{2}}(|\,0\,\rangle|\,a\,\rangle|\,b\,\rangle + |\,1\,\rangle|\,b\,\rangle|\,a\,\rangle) && (3) \\ &\mapsto \frac{1}{2}((|\,0\,\rangle + |\,1\,\rangle)|\,a\,\rangle|\,b\,\rangle + (|\,0\,\rangle - |\,1\,\rangle)|\,b\,\rangle|\,a\,\rangle) && (4) \\ &= |\,0\,\rangle\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle) + |\,1\,\rangle\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle). && (5) \end{aligned}$$

From the last expression we can see that the outcomes 0 and 1 are observed with probabilities

$$\begin{aligned} \text{Probability of } 0 &= \left|\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle)\right|^2 = \frac{1}{2}(1 + |\,\langle a|b\rangle\,|^2) \\ \text{Probability of } 1 &= \left|\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle)\right|^2 = \frac{1}{2}(1 - |\,\langle a|b\rangle\,|^2) \end{aligned}$$

The output state $|\,0\,\rangle\otimes$½$(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle) + |\,1\,\rangle\otimes$½$(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle)$ shows clearly that outcomes 0 or 1 lead to the "collapse" of the superposition to either the symmetric or the antisymmetric component of $|\,a\,\rangle|\,b\,\rangle$.

(c) [3 marks] [NEW] Outcome $M = 0$ occurs with probability $\frac{1}{2}(1 + |\,\langle a|b\rangle\,|^2)$ even when the two states are different. Outcome $M = 1$ can only occur if the two states are not identical.

(d) [5 marks] [NEW] You are essentially testing if the states of the two qubits are identical or not. Result $M = 0$ is inconclusive but $M = 1$ indicates that the two states are different. After many runs without $M = 1$ you can declare that the states are the same.

(e) [6 marks] [NEW] Projector $\frac{1}{2}(\mathbb{1} + S)$ projects on the symmetric subspace.

$$\Pr(0) = \mathrm{Tr}\left[\frac{1}{2}(\mathbb{1} + S)(\rho_a \otimes \rho_b)\right] = \frac{1}{2}\left[1 + \mathrm{Tr}\, S(\rho_a \otimes \rho_b)\right]$$

We first use the diagonal forms of the density matrices: $\rho_a = \sum_i p_i |\,a_i\,\rangle\langle\,a_i\,|$ and $\rho_b = \sum_j q_j |\,b_j\,\rangle\langle\,b_j\,|$ to show that

$$\mathrm{Tr}\, S(\rho_a \otimes \rho_b) = \sum_{ij} p_i q_j \,\mathrm{Tr}\, S(|\,a_i\,\rangle\langle\,a_i\,| \otimes |\,b_j\,\rangle\langle\,b_j\,|) = \sum_{ij} p_i q_j \,\mathrm{Tr}(|\,b_j\,\rangle\langle\,a_i\,| \otimes |\,a_i\,\rangle\langle\,b_j\,|),$$

which can be written as

$$\begin{aligned}\sum_{ij} p_i q_j |\langle a_i|b_j\rangle|^2 &= \sum_{ij} p_i q_j \langle a_i|b_j\rangle \langle b_j|a_i\rangle = \\ &= \sum_{ij}\sum_{c} p_i q_j \langle a_i|b_j\rangle \langle b_j|c\rangle \langle c|a_i\rangle = \\ &= \sum_{c}\sum_{ij} p_i q_j \langle c|a_i\rangle \langle a_i|b_j\rangle \langle b_j|c\rangle = \\ &= \mathrm{Tr}\left(\sum_i p_i |a_i\rangle\langle a_i|\right)\left(\sum_j q_j |b_j\rangle\langle b_j|\right) = \mathrm{Tr}\,\rho_a\rho_b.\end{aligned}$$

Hence

$$\Pr(0) = \frac{1}{2}(1 + \mathrm{Tr}\,\rho_a\rho_b).$$

(f) [3 marks] [NEW] No, it does not. The density operator $\rho \otimes \rho$ is not symmetric, i.e. it is not supported on the symmetric subspace. Indeed, the result $M = 1$, that is, a successful projection on the antisymmetric subspace, will occur with probability

$$\Pr(1) = \frac{1}{2}\left[1 - \mathrm{Tr}(\rho_a\rho_b)\right]$$

Now assume ρ_a and ρ_b are identical: $\rho_a = \rho_b \equiv \rho$. For a mixed state ρ, we have that $\mathrm{Tr}\,\rho^2 < 1$, hence

$$\Pr(1) = \frac{1}{2}(1 - \mathrm{Tr}\,\rho^2) > 0$$

for any mixed state ρ, even if $\rho \otimes \rho$ is not a symmetric state, that is, it is not a density matrix supported on the symmetric subspace.