Quantum Computing CO484

Tutorial*

Sheet 3 – Solutions

Exercise 1 *In the quantum teleportation network of Figure 1, the measurements of the first two qubits by Alice will collapse Bob's qubit as follows:*

$$00 \mapsto |\psi_3(00)\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$01 \mapsto |\psi_3(01)\rangle = \alpha|1\rangle + \beta|0\rangle$$

$$10 \mapsto |\psi_3(10)\rangle = \alpha|0\rangle - \beta|1\rangle$$

$$11 \mapsto |\psi_3(11)\rangle = \alpha|1\rangle - \beta|0\rangle$$

Alice communicates her two bits mn with Bob over a classical channel. Bob will then send his qubit through the circuit $X^n Z^m$ where

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Check that the final result $|\psi_4\rangle$ is indeed the state $|\psi_4\rangle = |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Solution

$$\mathbf{Z}^0\mathbf{X}^0 \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\mathbf{Z}^0\mathbf{X}^1 \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \mathbf{X} \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\mathbf{Z}^1\mathbf{X}^0 \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \mathbf{Z} \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\mathbf{Z}^1\mathbf{X}^1 \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

*Partly based on the tutorials by Abbas Edalat and Herbert Wiklicky.

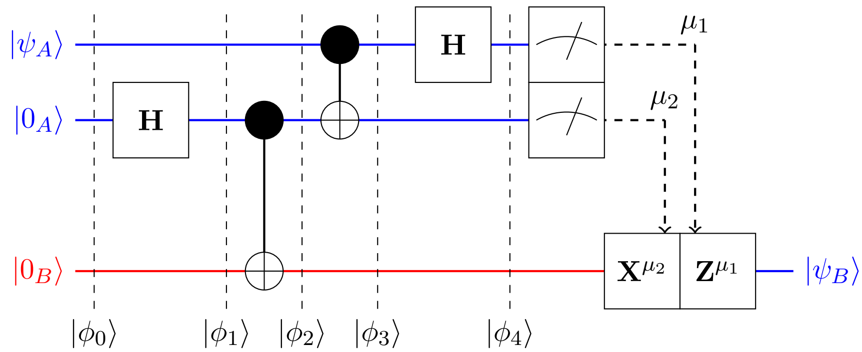

Figure 1: Quantum teleportation

Exercise 2 *Let be* $f : \{0,1\}^n \to \{0,1\}$ *and* $\mathbf{U}_f^n : \mathbb{C}^{n+1} \to \mathbb{C}^{n+1}$ *with*

$$\mathbf{U}_f^n : |\mathbf{x}, y\rangle \mapsto |\mathbf{x}, y \oplus f(\mathbf{x})\rangle \,,$$

as depicted in Figure 2. Check that for $n \in \mathbb{N}$ *the operator* $\mathbf{U}_f^n$ *is a unitary transformation.*

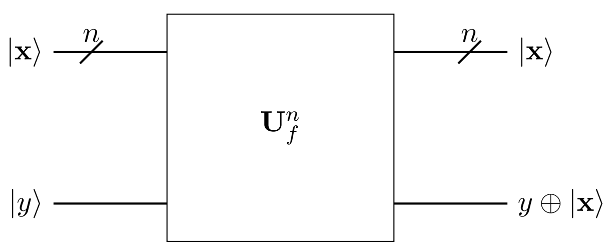

Figure 2: A gate for parallel computation

Solution For each $\mathbf{x} = x_1 \cdots x_n$ we have the two possible input qubits x_i0 and x_i1, which correspond to two adjacent rows of $\mathbf{U}_f$. The action of $\mathbf{U}_f$ on the these two basis vectors is to either leave them unchanged or swap them. Hence, the matrix $\mathbf{U}_f$ has the following two-by-two sub-matrix

$$\begin{pmatrix} 1 - f(x) & f(x) \\ f(x) & 1 - f(x) \end{pmatrix}$$

in the x_i0 and x_i1 row and column positions. Therefore, $\mathbf{U}_f$ induces a permutation of basis vectors and is thus unitary.

Exercise 3 *Show that*

$$\begin{aligned} \mathbf{H}\,|x\rangle &= \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}} (-1)^{xy}\,|y\rangle \\ \mathbf{H}^{\otimes n}\,|\mathbf{x}\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{[\mathbf{x},\mathbf{y}]}\,|\mathbf{y}\rangle \end{aligned}$$

where $[\mathbf{x},\mathbf{y}]$ *is the bitwise inner product of* $\mathbf{x}$ *and* $\mathbf{y}$ *modulo* 2.

Solution The first equality follows immediately by checking it for $x = 0$ and $x = 1$. As for the second, let $\mathbf{x} = x_1 x_2 \cdots x_n$. Then by the first equality we can write:

$$\mathbf{H}\,|x_i\rangle = \frac{1}{\sqrt{2}} \sum_{y_i\in\{0,1\}} (-1)^{x_i y_i}\,|y_i\rangle$$

Therefore, we get

$$\begin{aligned} \mathbf{H}^{\bigotimes n}\,|\mathbf{x}\rangle &= \bigotimes_{i=1}^{n} \mathbf{H}\,|x_i\rangle = \\ &= \bigotimes_{i=1}^{n} \frac{1}{\sqrt{2}} \sum_{y_i\in\{0,1\}} (-1)^{x_i y_i}\,|y_i\rangle = \\ &= \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} (-1)^{\sum_{i=1}^{n} x_i y_i}\,|\mathbf{y}\rangle = \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{[\mathbf{x},\mathbf{y}]}\,|\mathbf{y}\rangle\,. \end{aligned}$$

Exercise 4 **In order to distinguish a function* $f : \{0,1\}^n \to \{0,1\}$ *from constant to balanced with certainty, one needs at least* $2^{n-1}+1$ *classical queries. How many classical queries are sufficient for a success probability of* $p > \frac{1}{2}$*? What does this tell you about the Deutsch-Jozsa problem?*

Solution We can think of the Deutsch-Jozsa problem as follows. Alice randomly chooses an element x from a set with cardinal number $N = 2^n$ and sends it to Bob (for simplicity assume that N is even). Bob then applies a function $f : M \to \{0,1\}$, which is either constant or balanced. Afterwards Bob tells Alice $f(x)$. Classically Alice has to ask Bob $N/2+1$ times to know for sure if Bob's function is constant or balanced — in the worst case. But if she only wants to know it with probability $p \in (\frac{1}{2}, 1)$, she can do the following. Let k be the number of times that Alice asks Bob. If she gets at least one 0 and at least one 1 she knows for sure that Bob's function is balanced. If she gets the same value k times, she guesses that Bob's function is constant. It follows from elementary combinatorics that the probability that this strategy fails is given by

$$p_{\text{fail}} = \frac{2\binom{N/2}{k}}{\binom{N}{k}} = \frac{2\prod_{i=0}^{k-1}(N/2-i)}{\prod_{i=0}^{k-1}(N-i)} \ .$$

It follows that it is sufficient to choose k such that

$$1-p \geq \frac{2\prod_{i=0}^{k-1}(N/2-i)}{\prod_{i=0}^{k-1}(N-i)},$$

which is equivalent to

$$\log\left(\frac{1}{1-p}\right) \leq \sum_{i=0}^{k-1}\log\left(\frac{N-i}{N/2-i}\right) - 1.$$

Now, since

$$\sum_{i=0}^{k-1}\log\left(\frac{N-i}{N/2-i}\right) \geq k\cdot\log\left(\frac{N}{N/2}\right) = k\ ,$$

it is sufficient to choose

$$k = \left\lceil \log\left(\frac{1}{1-p}\right) + 1\right\rceil .$$

Remarkably, this is independent of N. Of course for $k \geq N/2+1$ the deterministic algorithm gives the answer with certainty. Note that we need randomness to implement the probabilistic algorithm. That is, the Deutsch-Jozsa problem is in **BPP** but not in **P**.

Notice that we can use a simpler strategy in order to compute the failure probability in the regime $k \leq N/2$. In fact, in this regime all the possible 2^k binary sequences of length k could be valid answers for Alice. Alice fails only in the correspondence of two binary sequences of length k: $0\dots0$ and $1\dots1$. Hence, the error probability is

$$p_{\text{fail}} = 1-p = \frac{2}{2^k} = 2^{1-k}$$

and the same conclusion as above holds.