Module CS406: *Research Directions in Computing*

Notes On Quantum Teleportation and Deutsch's Algorithm

by Nick Papanikolaou
Department of Computer Science
University of Warwick
nikos@dcs.warwick.ac.uk

The purpose of these notes is to detail the sequence of operations that take place in quantum teleportation, and to explain the steps in Deutsch's quantum algorithm. This material complements the CS406 lecture slides.

1 Quantum Teleportation

The process for teleporting a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $\alpha, \beta \in \mathbb{C}$, is shown in the form of a quantum circuit in Figure 1.

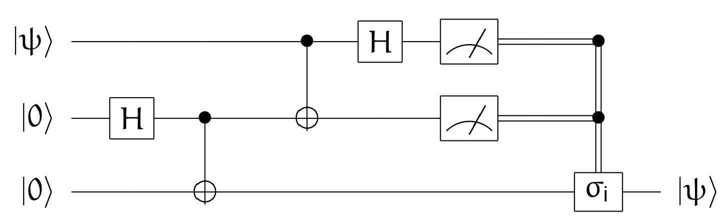

Figure 1: Quantum circuit diagram for the teleportation protocol. The value of i depends on the two measurement outcomes.

We will now go through each step in the circuit. The overall quantum state to start with is the tensor product of the three individual states; let's call this $|\psi_0\rangle$.

$$
\begin{aligned}
|\psi_0\rangle &= |\psi\rangle \otimes |0\rangle \otimes |0\rangle \\
&= (\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \\
&= \alpha|000\rangle + \beta|100\rangle
\end{aligned}
$$

A Hadamard gate is applied to the second qubit, which is equivalent to applying the operator $I \otimes H \otimes I$ to the state $|\psi_0\rangle$. This gives us $|\psi_1\rangle$.

$$
\begin{aligned}
|\psi_1\rangle &= (I \otimes H \otimes I)\,|\psi_0\rangle \\
&= \alpha \cdot (I \otimes H \otimes I)\,|000\rangle + \beta \cdot (I \otimes H \otimes I)\,|100\rangle \\
&= \alpha \cdot I|0\rangle \otimes H|0\rangle \otimes I|0\rangle + \beta \cdot I|1\rangle \otimes H|0\rangle \otimes I|0\rangle \\
&= \alpha \cdot |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \beta \cdot |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |110\rangle)
\end{aligned}
$$

Then the Controlled-Not gate is applied from the second to the third qubit, giving $|\psi_2\rangle$.

$$
\begin{aligned}
|\psi_2\rangle &= (I \otimes \mathbf{CNot})\,|\psi_1\rangle \\
&= \frac{\alpha}{\sqrt{2}}\left(I|0\rangle \otimes \mathbf{CNot}\,(|00\rangle) + I|0\rangle \otimes \mathbf{CNot}\,(|10\rangle)\right) + \\
&\quad + \frac{\beta}{\sqrt{2}}\left(I|1\rangle \otimes \mathbf{CNot}\,(|00\rangle) + I|1\rangle \otimes \mathbf{CNot}\,(|10\rangle)\right) \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle)
\end{aligned}
$$

The next step is to apply the Controlled-Not gate from the first to the second qubit, which transforms the quantum state into $|\psi_3\rangle$:

$$
\begin{aligned}
|\psi_3\rangle &= (\mathbf{CNot} \otimes I)\,|\psi_2\rangle \\
&= \frac{\alpha}{\sqrt{2}}(\mathbf{CNot}(|00\rangle) \otimes I\,|0\rangle + \mathbf{CNot}(|01\rangle) \otimes I\,|1\rangle) \\
&+ \frac{\beta}{\sqrt{2}}(\mathbf{CNot}(|10\rangle) \otimes I\,|0\rangle + \mathbf{CNot}(|11\rangle) \otimes I\,|1\rangle) \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle)
\end{aligned}
$$

Now, the Hadamard gate is applied to the first qubit, leading to state $|\psi_4\rangle$:

$$
\begin{aligned}
|\psi_4\rangle &= (H \otimes I \otimes I)\,|\psi_3\rangle \\
&= \frac{\alpha}{\sqrt{2}}\,(H\,|0\rangle \otimes (I \otimes I)\,|00\rangle + H\,|0\rangle \otimes (I \otimes I)\,|11\rangle) + \\
&\quad + \frac{\beta}{\sqrt{2}}(H\,|1\rangle \otimes (I \otimes I)\,|10\rangle + H\,|1\rangle \otimes (I \otimes I)\,|01\rangle) \\
&= \frac{\alpha}{\sqrt{2}}H\,|0\rangle \otimes (|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}H\,|1\rangle \otimes (|10\rangle + |01\rangle) \\
&= \frac{\alpha}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) \\
&= \frac{\alpha}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle + |001\rangle - |110\rangle - |101\rangle) \\
&= \frac{\alpha}{2}\,|000\rangle + \frac{\beta}{2}\,|001\rangle + \frac{\beta}{2}\,|010\rangle + \frac{\alpha}{2}\,|011\rangle + \frac{\alpha}{2}\,|100\rangle - \frac{\beta}{2}\,|101\rangle - \frac{\beta}{2}\,|110\rangle + \frac{\alpha}{2}\,|111\rangle \\
&= \frac{1}{2}\,|00\rangle \otimes (\alpha\,|0\rangle + \beta\,|1\rangle) + \frac{1}{2}\,|01\rangle \otimes (\alpha\,|1\rangle + \beta\,|0\rangle) + \\
&\quad + \frac{1}{2}\,|10\rangle \otimes (\alpha\,|0\rangle - \beta\,|1\rangle) + \frac{1}{2}\,|11\rangle \otimes (\alpha\,|1\rangle - \beta\,|0\rangle)
\end{aligned}
$$

The final form of the expression for state $|\psi_4\rangle$ makes it easy to identify the possible outcomes of measuring the first and the second qubit, which is what happens next. The first two qubits are in one of the four possible states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, and the state of the third qubit is respectively $\alpha\,|0\rangle + \beta\,|1\rangle$, $\alpha\,|1\rangle + \beta\,|0\rangle$, $\alpha\,|0\rangle - \beta\,|1\rangle$, $\alpha\,|1\rangle - \beta\,|0\rangle$.

Now, the first two qubits are measured, collapsing the state into one of four terms of the sum in $|\psi_4\rangle$.

If the measurement reduces the state of the first two qubits to $|00\rangle$, the third qubit is in state $|\psi\rangle$, so no further transformation is necessary (we just apply the identity operator, I). If the measurement gives $|01\rangle$, the third qubit is the same as $|\psi\rangle$ but with a ‘bit flip,’ so we need to apply operator X (a.k.a. σ_X) to it. In the third case, the third qubit is the same as $|\psi\rangle$ but with a ‘phase flip,’ so we need to apply operator Z (a.k.a. σ_Z) to it. In the fourth case, the third qubit is the same as $|\psi\rangle$ but with a ‘bit flip’ and a ‘phase flip,’ so we just apply operator $Y = XZ$ (a.k.a. σ_Y) to it. At the end, the state of the third qubit will be precisely $|\psi\rangle$, which is the state we started off with. Thus the state $|\psi\rangle$ is teleported from the first qubit to the third qubit.

Let $|\psi_5\rangle$ denote the state of the system after the first two have been measured. Then:

$$|\psi_5\rangle = \begin{cases} |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle), \text{ with probability } \frac{1}{4} \\ |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle), \text{ with probability } \frac{1}{4} \\ |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle), \text{ with probability } \frac{1}{4} \\ |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle), \text{ with probability } \frac{1}{4} \end{cases}$$

Now, let us denote the outcome of measuring the first qubit by A, and the outcome of measuring the second qubit by B (so that $A, B \in \{0, 1\}$). The final stage in the quantum teleportation circuit can be described as the following operation, which produces the ultimate quantum state $|\psi_6\rangle$:

$$|\psi_6\rangle = (I \otimes I \otimes Z^A X^B)\,|\psi_5\rangle$$

Notation 1 *The notation $Z^A X^B$ refers to the operator which results from multiplying (**not** tensoring) the operator Z to the power A, with the operator X to the power B. An operator raised to the power 0 is trivially the constant 1. The operator Y, which is by definition the product of Z and X, arises when $A = B = 1$. This notation allows us to express succinctly the choice of operator in the final step of quantum teleportation. See also [NC00].*

Example 1 *If measurement of the first two qubits leaves them in state $|10\rangle$, i.e. $A = 1$ and $B = 0$, then the operator $Z^1X^0 = Z$ is applied to the third qubit. Therefore the final state of the system, in this particular case, becomes:*

$$\begin{aligned} |\psi_6\rangle &= (I \otimes I \otimes Z)(|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle)) \\ &= (I \otimes I)\,|10\rangle \otimes Z(\alpha|0\rangle - \beta|1\rangle) \\ &= |10\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) \end{aligned}$$

and the third qubit has indeed taken on the initial state to be teleported.

2 Deutsch's Algorithm

The so-called Deutsch's problem is to determine whether a one-bit function $f : \{0, 1\} \longmapsto \{0, 1\}$ is **constant** or **balanced**. There are exactly four different functions with this signature; they are denoted f_1, f_2, f_3 and f_4 and they are defined in the table below.

Input, x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

From this table it can be seen that f_1 and f_4 are constant functions, i.e. $f_1(0) = f_1(1)$ and $f_4(0) = f_4(1)$. The functions f_2 and f_3 are balanced functions, and, in particular, we have $f_2(0) \neq f_2(1)$ and $f_3(0) \neq f_3(1)$.

In order to solve this problem classically, one has to evaluate the chosen function twice, once for each input. Deutsch's algorithm demonstrates how quantum parallelism can be used to solve the problem by evaluating the function only once. In what follows, we will go through the algorithm in a stepwise manner to see how it works; in particular, we will perform the calculations which arise in each step.

The algorithm can be expressed as a quantum circuit, which operates on two qubits in the initial state $|01\rangle$. The circuit consists of Hadamard gates, a so-called oracle U_f, and a single measurement. The circuit is illustrated in Figure 2. The quantum state of the two qubits at each stage in the circuit is labelled using the symbols $|\psi_0\rangle, \dots, |\psi_3\rangle$. A measurement of the first qubit is performed in the last stage of the circuit (not shown); if the outcome is 0, this indicates that the chosen function is constant. If the outcome of the final measurement is 1, it means that the chosen function is balanced.

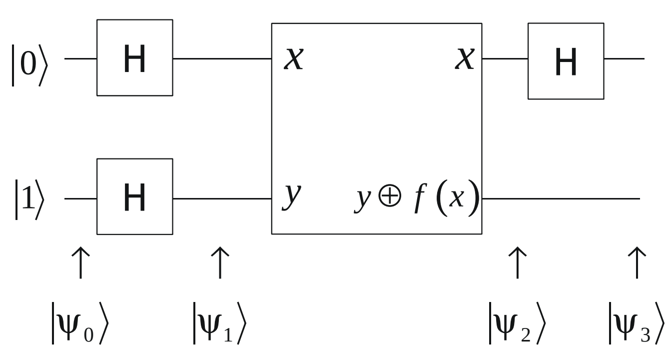

Figure 2: Circuit diagram for Deutsch's algorithm

The oracle, represented by the box in the middle of the circuit, is defined as the following quantum operator:

$$U_f : |x\rangle \otimes |y\rangle \longmapsto |x\rangle \otimes |y \oplus f(x)\rangle \text{, where } x, y \in \{0, 1\} \tag{1}$$

As you can see from this expression the operation U_f has the effect of flipping the second qubit if the first qubit is in state $|1\rangle$.

Notation 2 *We usually abbreviate tensor products of known qubit states by enclosing them in a single ket, e.g.* $|00\rangle$ *instead of* $|0\rangle \otimes |0\rangle$. *We can do this also when qubit states are unknown, but in this case a comma is used to separate the individual states in a ket; so we would write* $|x, y\rangle$ *instead of* $|x\rangle \otimes |y\rangle$ *. Thus, the definition of* U_f *above can be rewritten as*

$$U_f : |x, y\rangle \longmapsto |x, y \oplus f(x)\rangle$$

Notation 3 *The symbol* $\oplus$ *above denotes the exclusive-or operation (XOR) from boolean algebra. XOR is defined as follows:*

$$a \oplus b = \begin{cases} 0 \textit{ if } a = b \\ 1 \textit{ otherwise} \end{cases}$$

In order to understand the operation of the circuit, we could consider each of the functions f_1, f_2, f_3 and f_4 in turn. But we are going to do the calculations in the general case, independently of which f is chosen.

The input to the circuit is the state $|\psi_0\rangle = |01\rangle$. The Hadamard gate is applied to both qubits, leading to the quantum state $|\psi_1\rangle$:

$$\begin{aligned} |\psi_1\rangle &= (H \otimes H)\,|01\rangle \\ &= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$

The next step is the application of the oracle to $|\psi_1\rangle$. We use the definition of U_f to calculate the resulting state $|\psi_2\rangle$:

$$
\begin{aligned}
|\psi_2\rangle &= U_f\,|\psi_1\rangle \\
&= \frac{1}{2}(U_f\,|00\rangle - U_f\,|01\rangle + U_f\,|10\rangle - U_f\,|11\rangle) \\
&= \frac{1}{2}\left(|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle\right) \\
&= \frac{1}{2}\left[|0\rangle \otimes (\ |0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle\ ) + |1\rangle \otimes (\ |0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle\ )\right] \\
&= \frac{1}{2}\,|0\rangle \otimes (\ |0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle\ ) + \frac{1}{2}\,|1\rangle \otimes (\ |0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle\ )
\end{aligned}
$$

Next, we need to rewrite the state $|\psi_2\rangle$ in a more meaningful form; we have to use the following proposition.

Proposition 1 *For* $a \in \{0, 1\}$*:* $|0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a \cdot (|0\rangle - |1\rangle)$.

Proof. For $a = 0$ the LHS becomes $|0 \oplus 0\rangle - |1 \oplus 0\rangle = |0\rangle - |1\rangle$ and the RHS becomes $(-1)^0 \cdot (|0\rangle - |1\rangle) = |0\rangle - |1\rangle$, so both sides are indeed equal.

For $a = 1$ the LHS becomes $|0 \oplus 1\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle$ and the RHS becomes $(-1)^1 \cdot (|0\rangle - |1\rangle) = |1\rangle - |0\rangle$, so both sides are indeed equal. ∎

Using proposition 1, we obtain:

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\,|0\rangle \otimes (-1)^{f(0)} \cdot (|0\rangle - |1\rangle) + \frac{1}{2}\,|1\rangle \otimes (-1)^{f(1)} \cdot (|0\rangle - |1\rangle) \\
&= \left(\frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\right)\left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right)
\end{aligned}
$$

Look carefully at the above expression. Notice that the transformation does not seem to have affected the state of the second qubit, which has remained in the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. What is interesting is that the transformation U_f has introduced a so-called **phase kick-back** in the state of the first qubit; this is a fancy name for the factors $(-1)^{f(0)}$ and $(-1)^{f(1)}$. This trick/phenomenon comes up often in the study of quantum algorithms.

The final part of the algorithm only affects the state of the first qubit, which is now

$$
\frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle = (-1)^{f(0)}\left(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(0)\oplus f(1)}\,|1\rangle\right)
$$

For the next part of the calculation, we use the following proposition:

Proposition 2 *For* $a \in \{0,1\}$*:* $H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(-1)^a|1\rangle\right) = |a\rangle$.

Proof. For $a = 0$ the LHS becomes $H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = |0\rangle$ and the RHS becomes $|0\rangle$; both sides are indeed equal.

For $a = 1$ the LHS becomes $H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = |1\rangle$ and the RHS becomes $|1\rangle$; both sides are indeed equal. ■

The Hadamard gate is applied to the first qubit, taking the system to the quantum state $|\psi_3\rangle$:

$$\begin{aligned} |\psi_3\rangle &= (H \otimes I)|\psi_2\rangle \\ &= (-1)^{f(0)}\,|f(0) \oplus f(1)\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \end{aligned}$$

Finally, the first qubit is measured; the result is the value $f(0) \oplus f(1)$ with certainty. The value is 0 if f is constant and 1 if f is balanced. If you are not convinced, plug in a specific function $f : \{0,1\} \mapsto \{0,1\}$ of your choice into the formulae!

References

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Ashes Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[Gru99] Jozef Gruska. *Quantum Computing*. McGraw–Hill International, 1999.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[RP00] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non–physicists. ACM *Computing Surveys*, 32(3):300—335, 2000.