Lecture 4: Quantum Teleportation; Deutsch's Algorithm

January 26, 2006

Quantum teleportation

Suppose Alice has a qubit that she wants to send to Bob. Let us say that the state of the qubit is $\alpha\,|0\rangle + \beta\,|1\rangle$. How many classical bits would be required to accomplish this task?

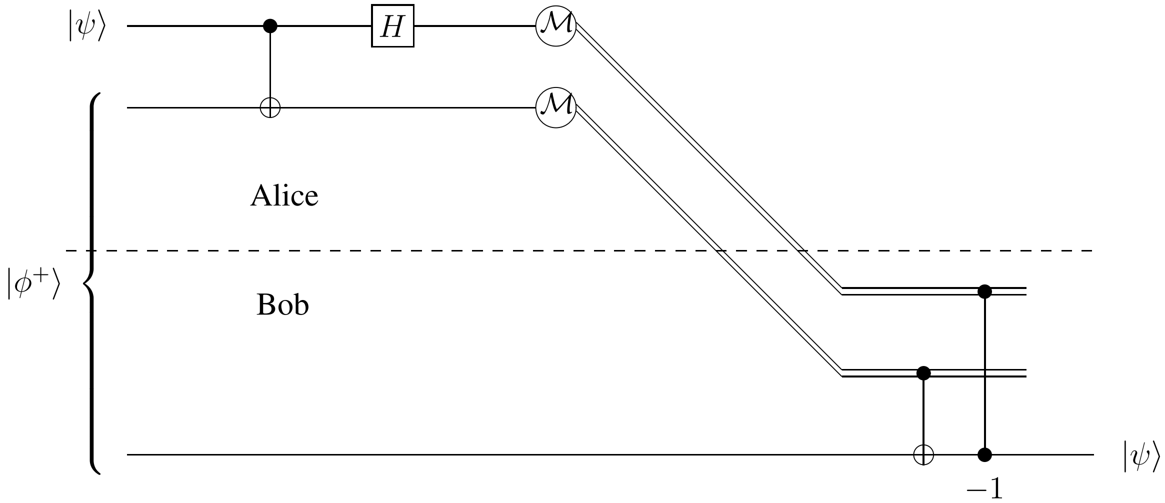
There are two reasonable answers to the question. The first answer is that the number of classical bits depends on the desired precision: α and β are arbitrary complex numbers (with $|\alpha|^2 + |\beta|^2 = 1$), but Alice could send approximations of α and β to Bob.

The second answer, which in some sense is the better answer, is that no number of classical bits of communication will suffice. Alice may not know α and β, and there is no way for her to perform measurements on her qubit that would reveal these numbers. Thus, she could not communicate this information to Bob because she could not even determine it for herself. There is also the possibility that Alice's qubit is entangled with one or more other qubits (in which case of course we would not be able to describe the state of the qubit as $\alpha\,|0\rangle + \beta\,|1\rangle$). Classical communication from Alice to Bob would not be able to somehow transmit this entanglement.

However, if we give Alice and Bob the additional resource of sharing an e-bit, just as in superdense coding, then it becomes possible for Alice to transmit a qubit to Bob using classical communication by means of *quantum teleportation*. Specifically, two bits of classical information will be needed to perform this task.

Quantum teleportation protocol

Here is the protocol described in terms of a quantum circuit diagram.



Let us assume that $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. The starting state is

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\left(\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle\right) = \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right).$$

First the CNOT gate is applied, which transforms the state to

$$\frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle\right).$$

Next, the Hadamard transform is applied, which transforms the state to

$$\begin{aligned}&\frac{1}{2}\left(\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|010\rangle - \beta\,|110\rangle + \beta\,|001\rangle - \beta\,|101\rangle\right)\\ &= \frac{1}{2}\,|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + \frac{1}{2}\,|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + \frac{1}{2}\,|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + \frac{1}{2}\,|11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle).\end{aligned}$$

Note that there have been no measurements or communication at this point. Bob's qubit *seems* to depend on α and β, but this is not really so. There would be no way for Bob to transform and measure his qubit alone at this point so that he would learn anything about α and β.

The state above has been expressed in a convenient way to determine the distribution of measurement outcomes and the resulting state of Bob's qubit after the measurements.

Case 1: Alice measures 00. This happens with probability

$$\left\|\frac{1}{2}(\alpha\,|0\rangle + \beta\,|1\rangle)\right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle).$$

Alice transmits the classical bits 00 to Bob. Because both bits are zero, he does not perform either of the two possible operations, and so his qubit remains in the state $\alpha\,|0\rangle + \beta\,|1\rangle$ at the end of the protocol.

Case 2: Alice measures 01. This happens with probability

$$\left\|\frac{1}{2}(\alpha\,|1\rangle + \beta\,|0\rangle)\right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle).$$

Alice transmits the classical bits 01 to Bob. Because the first transmitted bit is 0 and the second is 1, Bob performs a NOT operation on his qubit. Thus, the state of his qubit becomes $\alpha\,|0\rangle + \beta\,|1\rangle$.

Case 3: Alice measures 10. This happens with probability

$$\left\|\frac{1}{2}(\alpha\left|0\right\rangle - \beta\left|1\right\rangle)\right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$\left|10\right\rangle(\alpha\left|0\right\rangle - \beta\left|1\right\rangle).$$

Alice transmits the classical bits 10 to Bob. Because the first transmitted bit is 1 and the second is 0, Bob performs a σ_z operation on his qubit. Thus, the state of his qubit becomes $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$.

Case 4: Alice measures 11. This happens with probability

$$\left\|\frac{1}{2}(\alpha\left|1\right\rangle - \beta\left|0\right\rangle)\right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$\left|11\right\rangle(\alpha\left|1\right\rangle - \beta\left|0\right\rangle).$$

Alice transmits the classical bits 11 to Bob. Because both transmitted bits are 1, Bob first performs a NOT operation on his qubit, transforming it to $\alpha\left|0\right\rangle - \beta\left|1\right\rangle$, and then performs a σ_z gate to it, transforming it to the state $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$.

Thus, we see that in all four cases, Bob's qubit is in the state $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$ at the end of the protocol.

Something stronger is actually true. If Alice's initial qubit was entangled with other qubits, this entanglement will be preserved. In other words, teleportation works like a perfect quantum channel—it is exactly as if Alice had physically sent her qubit to Bob.

Deutsch's Algorithm

We have seen two interesting protocols that can be performed using quantum information: superdense coding and teleportation. Next, we will discuss various quantum algorithms, starting with a very simple one: Deutsch's Algorithm. This is a very different setting in which some advantage is gained by using quantum information over classical information.

Suppose that we have a device that computes some function $f : \{0,1\} \to \{0,1\}$. It is useful for the purposes of the present investigation to think of this device as a *black box*. This means that we cannot look inside the device to see how it works—the only way to gain information about the function f computed by the device is to give some input $a \in \{0,1\}$ and allow the device to output $f(a) \in \{0,1\}$. There are four possible functions from $\{0,1\}$ to $\{0,1\}$; let us call them f_0, f_1, f_2, and f_3.

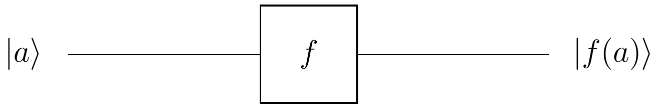
		f_0	f_1	f_2	f_3
Input	0	0	0	1	1
	1	0	1	0	1

Suppose that we are interested in determining which of the two possible alternatives holds:

1. f is **constant**, or
2. f is **balanced** (meaning each output appears the same number of times).

In particular, f_0 and f_3 are constant and f_1 and f_2 are balanced. Obviously two evaluations of the function are necessary and sufficient to answer the question. If only one evaluation is permitted, the function could still be either constant or balanced regardless of the input and output obtained.

Now let us consider the same question in the context of quantum information. We need to change the question slightly, however, in order for it to fit into the model of quantum information that we are considering. The change is that we need the black box to conform to a valid quantum operation. More specifically, we must insist that the action of the device corresponds to a unitary transformation. It is therefore **not** sufficient to consider the black box to be a one-qubit gate acting as follows:

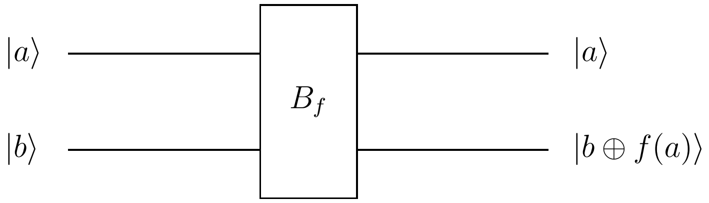


For example, if $f = f_0$ then this gate would correspond to the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

which is not unitary.

Instead, for any function $f : \{0,1\} \to \{0,1\}$ we define a 2-qubit quantum gate B_f as follows:



It can be verified that the corresponding matrix is unitary for any function f. For example, if $f = f_2$ from the table on the previous page, then $f(0) = 1$ and $f(1) = 0$, so the corresponding matrix is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For any function f, the matrix corresponding to B_f will always be a *permutation matrix*, meaning that all of the entries are 0 or 1 and every row and every column has exactly one 1 in it. Permutation matrices are always unitary.

In general, if

$$f : \{0,1\}^n \to \{0,1\}^m$$

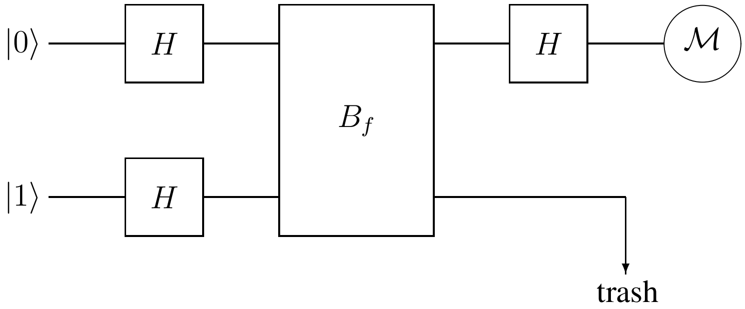
is any function (for any positive integers n and m), the associated quantum transformation B_f will be defined by

$$B_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle$$

(where $\oplus$ denotes the bitwise exclusive OR). The associated matrix will always be a permutation matrix, and is therefore unitary.

Getting back to the problem at hand, let us suppose that we have access to the transformation B_f for some $f : \{0,1\} \rightarrow \{0,1\}$, and the goal is the same as before: determine whether f is constant or balanced. Note that classically having access to B_f is no more helpful than access to f (both as black boxes)—two evaluations of B_f are necessary and sufficient to answer the question.

Using a quantum algorithm, however, it is only necessary to use one application of B_f to solve the problem. Here is a quantum circuit diagram explaining the procedure:



This procedure is known as *Deutsch's Algorithm*, and the problem of determining whether a one-bit function is constant or balanced is sometimes called *Deutsch's Problem*.

The output of the measurement is a single bit, and the interpretation is that the value 0 indicates that the function was constant and 1 indicates balanced. The qubit labeled trash is inconsequential at the end of the procedure. It is labeled trash only to highlight the (seemingly unusual) fact that it is not necessary to measure or do anything to it in order to determine the answer.

Let us analyze the algorithm to determine that it works correctly. Rather than taking the four cases separately, let us try to be more sophisticated and deal with the four cases all at the same time. The initial state is $\left|0\right\rangle \left|1\right\rangle$, and so the state after the first two Hadamard transforms is

$$\left(\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle\right)\left(\frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle\right).$$

We can partially expand this state as

$$\frac{1}{2}\left|0\right\rangle\left(\left|0\right\rangle - \left|1\right\rangle\right) + \frac{1}{2}\left|1\right\rangle\left(\left|0\right\rangle - \left|1\right\rangle\right).$$

Performing the B_f operation transforms this state to

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

Here we have used the fact that

$$\left|0\oplus a\right\rangle - \left|1\oplus a\right\rangle = (-1)^a(\left|0\right\rangle - \left|1\right\rangle)$$

for $a \in \{0,1\}$.

Notice that something seemingly strange has happened. The B_f transformation has apparently not changed the state of the second qubit; it has remained in the state

$$\frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle.$$

There has been an important effect, however, which is that the factors $(-1)^{f(0)}$ and $(-1)^{f(1)}$ have appeared in the state of the first qubit. This phenomenon is sometimes known as “phase kick-back”. It is a commonly used trick in quantum algorithms.

At this point the second qubit is thrown in the trash, which should not bother us because we know that its state is completely independent from the state of the first qubit; we know that its state is $\frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle$, regardless of the choice of f. This leaves the first qubit in the state

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

which we can write as

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

The final Hadamard transform takes this state to

$$(-1)^{f(0)}\left|f(0)\oplus f(1)\right\rangle.$$

Here we have used the observation that

$$H\left(\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}(-1)^a\left|1\right\rangle\right) = \left|a\right\rangle$$

for $a \in \{0,1\}$, which is again easily verified by considering the cases $a = 0$ and $a = 1$. The measurement therefore results in the value $f(0) \oplus f(1)$ with certainty. This value is 0 if f is constant and 1 if f is balanced.