Quantum Teleportation Protocol

Paweł Pamuła

December 23, 2012

Abstract

A brief description of relatively simple quantum teleportation protocol, which allows transmiting a qubit from one place to another, without physically transferring it through the space.

1 Qubit

Qubit is a linear superposition of two arbitralily chosen orthonormal basis vectors.

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

Unit vector $|0\rangle$ is $[1,0]^T$ and $|1\rangle$ is $[0,1]^T$. α_0 and α_1 denote *probability amplitudes* and they are complex numbers in general. Probability of outcome $|0\rangle$ is $|\alpha_0|^2$ and $|1\rangle$ is $|\alpha_1|^2$. $|\psi\rangle$ is an unit vector from two-dimensional Hilber space $\mathcal{H}$, therefore $|\alpha_0|^2 + |\alpha_1|^2 = 1$. It is consistent with our empirical intuiton - after measurment one obtains a well-defined state $|0\rangle$ or $|1\rangle$ and there is no other possibility.

To measure a state we have to choose an orthonormal basis and probability of the outcome is equal to the square of the length of a projection onto basis vector. After measurement state collapses to the basis vector.

We can perform measurments in arbitralily chosen basis. For instance, *sign basis* is defined as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and $|\psi\rangle$ can be eassily rewritten in this basis as

$$|\psi\rangle = \frac{\alpha_0 + \alpha_1}{\sqrt{2}}|+\rangle + \frac{\alpha_0 - \alpha_1}{\sqrt{2}}|-\rangle$$

2 Composite systems

State of composite system consisting of two qubits is described as a tensor product of two states. Suppose the first qubit is in state $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and second is $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. We can interpret composite state $|\psi\rangle$ which is equal to $|\psi_1\rangle \otimes |\psi_2\rangle$ as $|\psi_1\psi_2\rangle$.

$$\begin{aligned}|\psi\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\end{aligned} \tag{1}$$

Given two independent qubits, we can always obtain state of such composite system. But it is not always possible to obtain tensor product from two-qubit state. Suppose there is state $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. We would like to rewrite as $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$. According to (1), $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}$ and $\alpha_1\beta_1 = \frac{1}{\sqrt{2}}$, therefore $\alpha_0, \alpha_1, \beta_0, \beta_1 \neq 0$. On the other hand $\alpha_0\beta_1 = 0$, which obviously is a contradiction - we cannot factorize those kind of states called *entangled states*.

We can perform partial measurment on such composite systems. For example, we can measure only the first qubit and obtain $|0\rangle$ with probability $P[|0\rangle]$ and $|1\rangle$ with probability $P[|1\rangle]$

$$P[|0\rangle] = |\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2$$

$$P[|1\rangle] = |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2$$

After measurment there is a new state.

$$|\mathbf{0}\psi'\rangle = \frac{1}{\sqrt{|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2}}(\alpha_0\beta_0|\mathbf{00}\rangle + \alpha_0\alpha_1|\mathbf{01}\rangle)$$

There are four states which represent the simplest examples of entanglement of two qubits called *Bell states*.

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Bell states have this interesting property - two qubits that are in entangled state can be spatially separated but they are not subject to relativistic limitations. When someone measures the first qubit there are two possible outcomes. In each case, any subsequent measurement in the same basis will always return the same result with certainity.

3 Evolution of a qubit

Evolution of qubit can be described as a rotation of an unit vector in two-dimensional Hilbert space. Transformation can be represented by operators applied to a vector. Those operators are unitary, therefore they preserve the angles between vectors and their lengths. We can think of those transformation as quantum gates. A gate which acts k one qubit is represented by $2^k \times 2^k$ matrix. There are three basic one-qubit gate necessary to describe quantum teleportation protocol.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

X is equal to a rotation around X-axis by π radians.

$$X(\alpha_0|0\rangle + \alpha_1|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} =$$
$$= \alpha_1|0\rangle + \alpha_0|1\rangle$$

Z is called phase flip and it is equal to a rotation around Z-axis by π radians.

$$Z(\alpha_0|0\rangle + \alpha_1|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ -\alpha_1 \end{bmatrix} =$$
$$= \alpha_0|0\rangle - \alpha_1|1\rangle$$

H is called Hadamard gate and it changes the basis from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$ and the other way around.

$$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$
$$= \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha_0 + \alpha_1 \\ \alpha_0 - \alpha_1 \end{bmatrix} =$$
$$= \frac{\alpha_0 + \alpha_1}{\sqrt{2}}|0\rangle - \frac{\alpha_0 - \alpha_1}{\sqrt{2}}|1\rangle$$

One application of the Hadamard gate to either a 0 or 1 qubit will produce a quantum state that, if observed, will be a 0 or 1 with equal probability.

There are gates acting or two cubits, where one of them act as a control for operation. One of them example is CNOT (controlled NOT) gate.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

This particular CNOT gate takes the first bit as a control bit and if it is equal to 1 it flips the second one.

We can combine those gates in more complicated circuits. Let's consider circuit involving Hadamard and CNOT gate and input state $|00\rangle$

It maps the first bit to $|+\rangle$ and performs control not using first bit as control.

$$|00\rangle \longrightarrow \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{|+\rangle} |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The result is a previously mentioned Bell state. by varying the input we can obtain other three Bell states, which proves, that using basic quantum gates we are able to produce entangled states.

4 No-cloning theorem

Suppose our task is to construc a quantum circuit that accepts 2 qubits at the input - one is unknown superposition of 2 states (α_0 and α_1 are unknown, obtained as a result of an experiment for instance) and $|s\rangle$ is a well-known state, such as $|0\rangle$.

When $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, by linearity of unitary operator U we obtain:

$$U[(\alpha_0|0\rangle + \alpha_1|1\rangle)|s\rangle] = \alpha_0 \underbrace{U|0\rangle|s\rangle}_{|00\rangle} + \alpha_1 \underbrace{U|1\rangle|s\rangle}_{|11\rangle}$$

U is construct in a such way, that $U|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle$. On the other hand output is a tensor product of two states $|\psi\rangle$.

$$|\psi\psi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle)$$
$$= \alpha_0^2|00\rangle + \alpha_0\alpha_1|01\rangle + \alpha_1\alpha_0|10\rangle + \alpha_1^2|11\rangle$$

which obviously is a contradiction. We conclude, that there is no such quantum circuit, that can clone an unknown quantum state.

5 Quantum teleportation

Quantum teleportation protocol is based on basic one and two-qubit gates. Prerequisites for this protocol are an unknown qubit, entangled state shared between sender and receiver and a set of quantum gates. Assume Alice (sender) has an uknown qubit - coefficients α_0, α_1 are unknown. She would like Bob to have this state, for example to continue an experiment using some devices located in another place.
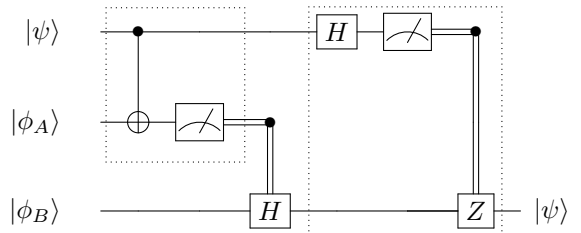
Let's consider first group of gates. Alice has $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and one of two qubits $|\phi_A\rangle$ in entagled state.

1) In the first step, Alice performs CNOT operation with first bit as a control bit and second one as a result bit.

$$CNOT|\psi\rangle|\phi_A\rangle = \frac{\alpha_0}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\alpha_1}{\sqrt{2}}(|100\rangle + |111\rangle)$$

Following result:

$$|\psi\rangle|\phi_A\rangle = \frac{\alpha_0}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\alpha_1}{\sqrt{2}}(|110\rangle + |101\rangle)$$

2) Alice measures the second bit in the composite system. There are two possible results

$$0 \longrightarrow (\alpha_0|00\rangle + \alpha_1|11\rangle)$$
$$1 \longrightarrow (\alpha_0|01\rangle + \alpha_1|10\rangle)$$

In the second case Alice contacts Bob through classical medium and tells him to apply bit flip (X) gate.

3) Alice applies Hadamard gate to the first bit in the composite system.

$$\frac{\alpha_0}{\sqrt{2}}(|+\rangle + |-\rangle)|0\rangle + \frac{\alpha_1}{\sqrt{2}}(|+\rangle - |-\rangle)|1\rangle =$$
$$\frac{1}{\sqrt{2}}|+\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle) + \frac{1}{\sqrt{2}}|-\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle)$$

4) Alice performs measurement in sign basis. If the results is $|+\rangle$ entangled state is set to initial $|\psi\rangle$. In other case she contacts Bob, who should apply phase flip (Z) gate. It turns out that Bob has initial unknown state $|\psi\rangle$.

6 Summary

First of all, this protocol does not violate no-cloning theorem, because Alice measures both her bits and after measurment they are destroyed. Information also does not violate theory of relativity, because Bob has to receive message via classical medium how to apply X and Z gate. As the result Bob receives initial unknown states $|\psi\rangle$.