Chapter 6: Quantum Protocols

Jessica John Britto
Indian Institute of Technology Kharagpur

June 18, 2022

1 Introduction

Product States are those states which can be written as tensor products of single qubits and are not correlated. **Entangled states** are those states which cannot be written as tensor product of single qubits and are maximally entangled such as the Bell states. **Partially Entangled states** cannot be factored into tensor products of single qubits, however, they are not completely correlated, i.e, having knowledge about half the pair of a state such this, will not assist us in drawing complete information about the other half.

Maximum entanglement is possible between two qubits. In case of partial entanglement, then the correlation is possible between more than two parties. In this case, the quantum states are expressed using density matrices since they are a probabilistic mixtures of kets.

2 Superdense coding

In **Superdense coding**, two classical bits of information is passed through a single qubit. An entangled state is shared between two parties, namely Alice and Bob, each has one qubit of the entangled state.

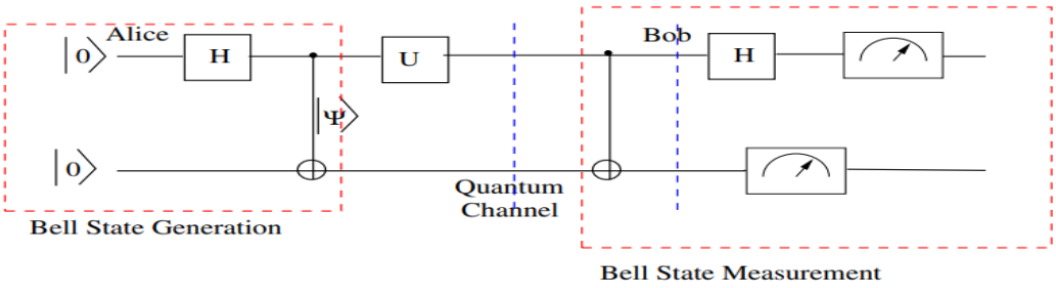


Figure 1: Circuit Diagram of Superdense Coding

Alice will perfom local operations on her qubit depending on the information she wants to send and then the qubit is sent to Bob through a quantum channel. Bob, after receiving this, will decode the transferred information. The following operations will be undertaken depending on which one of these information that Alice wants to send - $00, 01, 10, 11$.

1. If 00 cbit is to be sent, then no operation is performed by Alice on the bell state - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

2. If 01 cbit is to be sent, then the X operator is performed by Alice on the first qubit of the bell state - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to get $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$
3. If 10 cbit is to be sent, then the iY operator is performed by Alice on the first qubit of the bell state - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to get $\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle)$
4. If 11 cbit is to be sent, then the Z operator is performed by Alice on the first qubit of the bell state - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to get $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

cbit to be sent	Action by Alice	Resulting state
00	No action by Alice	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	Alice applies $X \otimes I$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
10	Alice applies $iY \otimes I$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
11	Alice applies $Z \otimes I$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

In order to decode the message, Bob applies $CNOT$ gate on Alice's qubit and gets the followign results as tabulated below.

cbit to be sent	state Bob has	Result of CNOT
00	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$
01	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$
10	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$
11	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$

After receiving it through the quantum channel and gets the following w.r.t the previously stated cases above -

1. For 00, it is $|+\rangle\,|0\rangle$
2. For 01, it is $|+\rangle\,|1\rangle$
3. For 10, it is $|-\rangle\,|1\rangle$
4. For 11, it is $|-\rangle\,|0\rangle$

Now, Bob does measurement on the second qubit, then applies the hadamard gate to the first qubit and measures its value. We get the following -

1. For 00, it is $|0\rangle \otimes |0\rangle$
2. For 01, it is $|0\rangle \otimes |1\rangle$
3. For 10, it is $|1\rangle \otimes |1\rangle$
4. For 11, it is $|1\rangle \otimes |0\rangle$

3 Quantum Teleportation

No-cloning theorem - A quantum state cannot be cloned since if such an operator were to exist, then it cannot clone all the quantum states. It can only clone quantum states which are orthogonal to each other or they are the same. Hence, cloning of quantum state is not possible.

In quantum teleportation, information of a quantum state $|k\rangle$ has to be shared through the entangled stated between Alice and Bob. Each has one qubit of the entangled bell state - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The information about the quantum state is communicated through a classical communication channel. Alice has two qubits with her - qubit 1 is $|k\rangle$ and qubit 2 is the one pair of the entangled state while Bob has the other half which is the qubit 3.

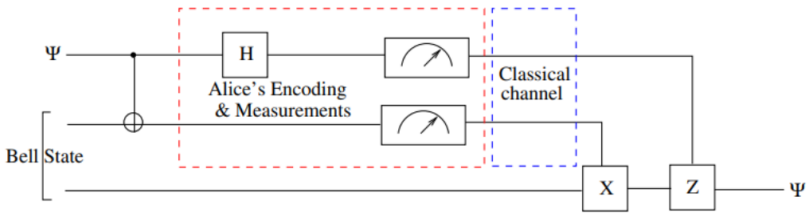


Figure 2: Circuit Diagram of Quantum Teleportation

Now, Alice applies a $CNOT$ gate with target as qubit 2 and control as qubit 1, followed by operating hadamard gate on qubit 1. Then, Alice measures both the qubits 1 and 2, hence the state collapses to one of the following and the measurements are communicated to Bob through a classical communication channel.

1. $a\,|0\rangle + b\,|1\rangle$ if the measurements give 00.
2. $a\,|1\rangle + b\,|0\rangle$ if the measurements give 01.
3. $a\,|0\rangle - b\,|1\rangle$ if the measurements give 10.
4. $a\,|1\rangle - b\,|0\rangle$ if the measurements give 11.

Bob reconstructs Alice's state by applying no operation on the qubit he has in case 1. In case 2, applies X operator on it. In case 3, applies a Z operator and in case 4, ZX operator.

In this case, information is communicated using a classical channel, hence, the information is not transmitted faster than the speed of light.
No-cloning theorem is not violated since Alice has either state $|0\rangle$ or $|1\rangle$ in place of $|k\rangle$ while Bob has lost his state while reconstructing $|k\rangle$.

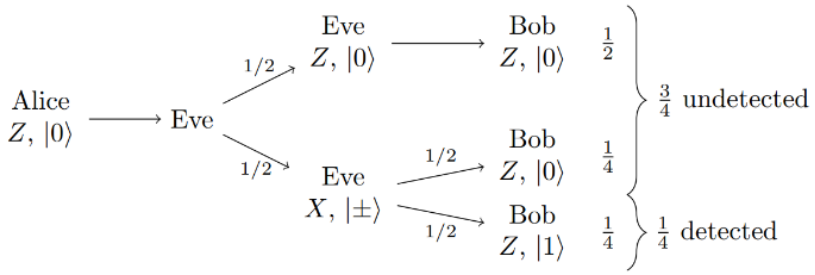
4 Quantum Key Distribution

Using BB-84 protocol, we can generate secret keys to be shared between two parties, Alice and Bob, with a third party, named Eve, trying to get information about the key. The key is used for encrypting messages. Hence, the secrecy of the key becomes important. Eve cannot measure the key since it will collapse to a value determined by her device and she cannot copy the state due to no-cloning theorem and the states are not orthogonal. Hence, in both the cases, the protocol can be aborted when suspected Eve is watching, hence Eve cannot gain significant information about the key.

In this protocol, two bases are used to encode $|0\rangle$ and $|1\rangle$ using photons. These two bases are H/V (called the computational basis, denoted by H) and angle of 45° with horizontal/ angle of 135° with horizontal (called the diagonal basis, denoted by D). Alice uses these two bases randomly encode the key and takes note of it. Then, she sends the qubits through a quantum network. Bob follows the same. Bob does not have knowledge about the bases Alice has used to encode each bit in the key. On doing so randomly, it turns that Bob encodes the bits correctly about 75% the time. This is

possible because half the time, Bob encodes the same basis and a quarter time due to probabilistic reasons. The cases in which the bases do not agree will be discarded.

Assuming Eve is secretly measuring the bits and then resends to Bob, then in this case, Bob decodes the bits correctly irrespective of the basis 75% and decodes incorrectly $\frac{1}{4}$ times. Supposing Alice and Bob generate k bits, and compare n (n¡¡k) bits randomly to detect the presence of Eve. Then, in this case, the presence of Eve is undetected is $(\frac{3}{4})^n$ and the probability of Eve being detected is $1 - (\frac{3}{4})^n$ which is close to 0.99999...



5 References

1. Chapter 6 from "Introduction to Classical and Quantum Computing"
2. Topics 6 and 7 from Lecture Notes of Professor D K Ghosh
3. Quantum Protocols and Algorithms from Qiskit