Qubits

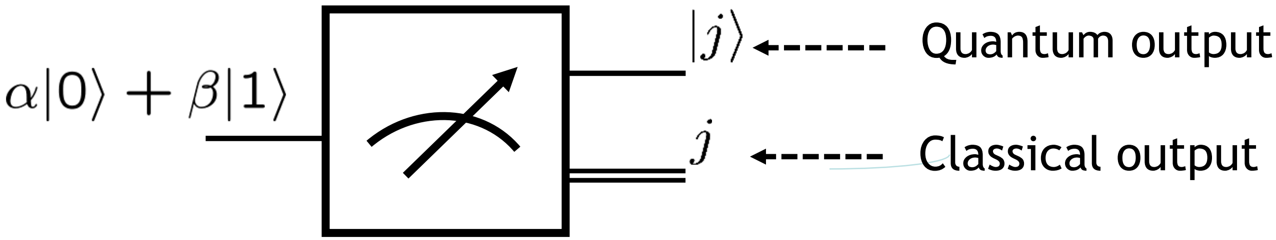
A **qubit** is a physical object (for instance, elementary particle) with two "orthogonal" states, typically denoted by $|0>$ and $|1>$. Like the spin (spin up is $|0>$ and spin down is $|1>$), or low and high electron orbits in a atom.

For quantum computing it is convenient to abstract from a particular physical realization of qubit and use a mathematical definition for it.

Def. A *pure quantum state* of qubit is a unit norm vector $|v\rangle \in \mathbb{C}^2, \ \ || \, |v\rangle \, || = 1$, i.e.

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle, \ \ \alpha, \beta \in \mathbb{C}, \ \ |\alpha|^2 + |\beta|^2 = 1$$

Measurement of $|v>$ (with respect to $|0>$ and $|1>$)



Measurement (special case) During the measurement of the quantum state $|v>$ it collapses either to $|0>$ or $|1>$. The Classical Output shows us to which state ($|0>$ or $|1>$) $|v>$ collapsed. Q. mechanics predicts the probabilities of collapsing to $|0>$ and $|1>$:

Cl. Output	**Q. Output**	**Probability**
$j=0$	$\|j>=\|0>$	$\|\alpha\|^2$
$j=1$	$\|j>=\|1>$	$\|\beta\|^2$

Let us assume that we have n qubits 

Postulate 1 *A pure state of n qubits* is a unit vector $|v\rangle \in \mathbb{C}^{2^n}$, i.e.,

$$|v\rangle = \alpha_{0\ldots00}|0\ldots00\rangle + \alpha_{0\ldots01}|0\ldots01\rangle + \ldots + \alpha_{1\ldots11}|1\ldots11\rangle$$

$$|\alpha_{0\ldots00}|^2 + |\alpha_{0\ldots01}|^2 + \ldots + |\alpha_{1\ldots11}|^2 = 1$$

An overall phase rotation does not change the state, so the vectors $|v\rangle$ and $e^{i\psi}|v\rangle$, $i^2 = \sqrt{-1}$, define the same quantum state

Arithmetic Rules for Dirac notations

Multiplication:

$$|0\rangle|1\rangle = |01\rangle, \;\; |0\rangle|00\rangle = |000\rangle$$

We can combine like terms:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|00\rangle = (\alpha + \gamma)|00\rangle + \beta|01\rangle$$

We can factor out:

$$\alpha|0010\rangle + \beta|0011\rangle = |00\rangle(\alpha|10\rangle + \beta|11\rangle)$$

If we have two qubits:

$$\underset{1}{\alpha|0\rangle + \beta|1\rangle} \qquad \underset{2}{\gamma|0\rangle + \delta|1\rangle}$$

Then their joint state is obtained as the product:

$$(\alpha|0\rangle+\beta|1\rangle)(\gamma|0\rangle+\delta|1\rangle) = \alpha\gamma|00\rangle+\alpha\delta|01\rangle+\beta\gamma|10\rangle+\beta\delta|11\rangle$$

Qubits may have a joint state that is not representable as a product of individual states, for example

$$\frac{1}{\sqrt{2}}(|00\rangle + \delta|11\rangle)$$

In this case we say that these qubits are *entangled*, or that this is an *entangled state*.

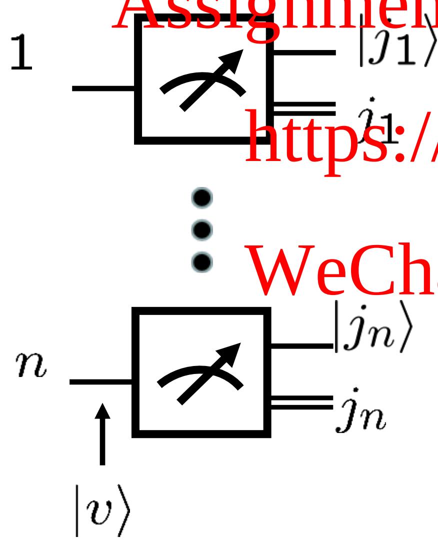
Example 1 A generic quantum state of 3 qubits has the form

$$|v\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \ldots + \alpha_{111}|111\rangle$$

If, for example, all the coefficients are $1/\sqrt{8}$ we have the state

$$|v\rangle = 1/\sqrt{8}(|000\rangle + |001\rangle + \ldots + |111\rangle)$$

Measurement of *n* Qubits.



The joint state of *n* qubits before the measurement is

$$|v\rangle = \alpha_{0\ldots00}|0\ldots00\rangle + \alpha_{0\ldots01}|0\ldots01\rangle + \ldots + \alpha_{1\ldots11}|1\ldots11\rangle$$

Postulate 2 Upon the measurement each qubit collapses either to $|0>$ or $|1>$. The probabilities of the classical and quantum outcomes are

Cl. Output	**Q. Output**	**Probability**
$j_1, \ldots, j_n$	$\|j_1\rangle, \ldots, \|j_n\rangle$	$\|\alpha_{j_1,\ldots,j_n}\|^2$

Example 2 Let 2 qubits have the state

$$|v\rangle = 0.2|00\rangle + 0.4|01\rangle + \sqrt{0.8}|11\rangle$$

Note that $0.2^2 + 0.4^2 + (\sqrt{0.8})^2 = 1$

The possible results of the measurement with the corresponding probabilities are

Cl. Output	**Q. Output**	**Probability**
0 0	$\|0\rangle \quad \|0\rangle$	0.04
0 1	$\|0\rangle \quad \|1\rangle$	0.16
1 0	$\|1\rangle \quad \|0\rangle$	0
1 1	$\|1\rangle \quad \|1\rangle$	0.8

Using Postulate 2, we can find the probability whether the *m*-th qubit will collapse to $|0>$ (or to $|1>$). We simply sum up the probabilities of all the outputs in which the *m*-th qubit collapses to $|0>$ (or to $|1>$).

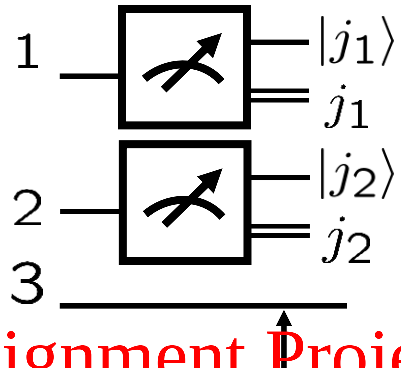
Cl. Output	**Q. Output**	**Probability**
$j_m = 0$	$\lvert j_m\rangle = \lvert 0\rangle$	$\displaystyle\sum_{j_1\ldots j_n : j_m = 0} \lvert\alpha_{j_1\ldots j_n}\rvert^2$

this is summation over all possible binary values of $j_1 \ldots j_n$, but always with $j_m = 0$

In **Example 2** we have

Cl. Output	**Q. Output**	**Probability**
$j_1 = 0$	$\lvert j_1\rangle = \lvert 0\rangle$	$\lvert\alpha_{00}\rvert^2 + \lvert\alpha_{01}\rvert^2 = 0.2^2 + 0.4^2 = 0.2$
$j_1 = 1$	$\lvert j_1\rangle = \lvert 1\rangle$	$\lvert\alpha_{10}\rvert^2 + \lvert\alpha_{11}\rvert^2 = 0^2 + 0.8 = 0.8$
$j_2 = 0$	$\lvert j_2\rangle = \lvert 0\rangle$	$\lvert\alpha_{00}\rvert^2 + \lvert\alpha_{10}\rvert^2 = 0.2^2 + 0^2 = 0.04$
$j_2 = 1$	$\lvert j_2\rangle = \lvert 1\rangle$	$\lvert\alpha_{01}\rvert^2 + \lvert\alpha_{11}\rvert^2 = 0.4^2 + 0.8 = 0.96$

Postulate 2 (continued) What if we measure only *m* of *n* qubits? We consider the case of measuring 2 of 3 qubits: (you will be able to generalize it to any other case)



$|\psi\rangle$ is the joint quantum state of all 3 qubits after the measurement

Each of the first 2 qubits collapses (either to $|0>$ or $|1>$). The 3-rd qubit does not collapse. Classical and quantum outcomes, and the corresponding probabilities are

Cl. Output	**Q. Output**	**Probability**
$j_1 = 0, j_2 = 0$	$\|\psi\rangle = \gamma(\alpha_{000}\|000\rangle + \alpha_{001}\|001\rangle)$	$\|\alpha_{000}\|^2 + \|\alpha_{001}\|^2$
	$= \|00\rangle(\gamma\alpha_{000}\|0\rangle + \gamma\alpha_{001}\|1\rangle),$	
	$\gamma = 1/\sqrt{\|\alpha_{000}\|^2 + \|\alpha_{001}\|^2}$	

Here γ is a normalization factor to insure that $|| \; |\psi\rangle \; || = 1$ (see Postulate 1).

Note that the 3-rd qubit is in the state: $\gamma\alpha_{000}|0\rangle + \gamma\alpha_{001}|1\rangle$

Cl. Output	**Q. Output**	**Probability**
$j_1 = 0, j_2 = 1$	$\|\psi\rangle = \gamma(\alpha_{010}\|010\rangle + \alpha_{011}\|011\rangle)$ $= \|01\rangle(\gamma\alpha_{010}\|0\rangle + \gamma\alpha_{011}\|1\rangle),$ $\gamma = 1/\sqrt{\|\alpha_{010}\| + \|\alpha_{011}\|^2}$	$\|\alpha_{010}\|^2 + \|\alpha_{011}\|^2$
$j_1 = 1, j_2 = 0$	$\|\psi\rangle = \|10\rangle(\gamma\alpha_{100}\|0\rangle + \gamma\alpha_{101}\|1\rangle),$ $\gamma = 1/\sqrt{\|\alpha_{100}\| + \|\alpha_{101}\|^2}$	$\|\alpha_{100}\|^2 + \|\alpha_{101}\|^2$
$j_1 = 1, j_2 = 1$	$\|\psi\rangle = \|11\rangle(\gamma\alpha_{110}\|0\rangle + \gamma\alpha_{111}\|1\rangle),$ $\gamma = 1/\sqrt{\|\alpha_{110}\| + \|\alpha_{111}\|^2}$	$\|\alpha_{110}\|^2 + \|\alpha_{111}\|^2$

Def. A linear operator (matrix) U is unitary iff $U^{-1} = U^{\dagger}$.

Example 3

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix},\ U^{\dagger} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix},\ UU^{\dagger} = I_2$$

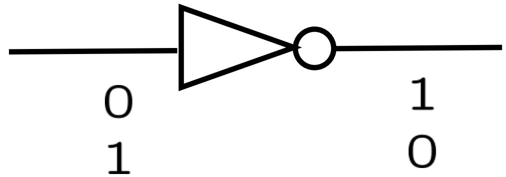
Postulate 3 The evolution of a closed quantum system is described by a unitary operator.

Time	**Quantum State**
t_1	$\vert v\rangle$
t_2	$\vert v'\rangle = U\vert v\rangle$

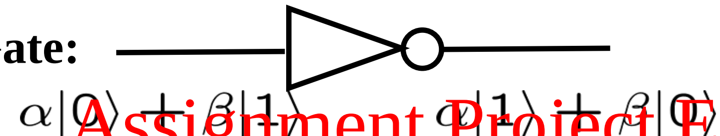
Note that U depends on t_1, t_2

Quantum Circuits

Classical Not Gate:



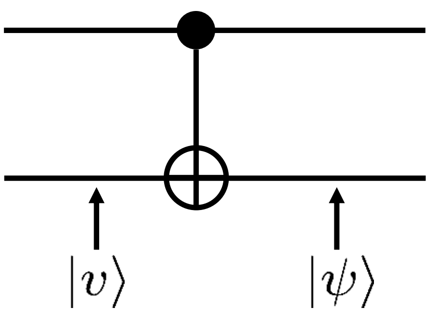
Quantum Not Gate:



The corresponding unitary operator:

$$U_{NOT} = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Quantum CNOT (control not) Gate (analog of classical XOR)



The joint state of 2 qubits before the gate is

$$|v\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

CNOT flips 2-nd qubit if 1-st qubit is 1, that is in each $|ab\rangle$ it flips b if a = 1.

The state after the gate is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$$

Unitary operator of CNOT gate is

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Indeed, in linear algebra notation we have

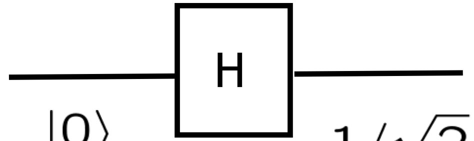
$$|v\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Switching from Dirac's notations to linear algebra notations and back, we get

$$U_{CNOT}|v\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \\ \alpha_{10} \end{pmatrix}$$

$$= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle = |\psi\rangle$$

Hadamard Gate:



$|0\rangle$ $\quad 1/\sqrt{2}(|0\rangle + |1\rangle)$

$|1\rangle$ $\quad 1/\sqrt{2}(|0\rangle - |1\rangle)$

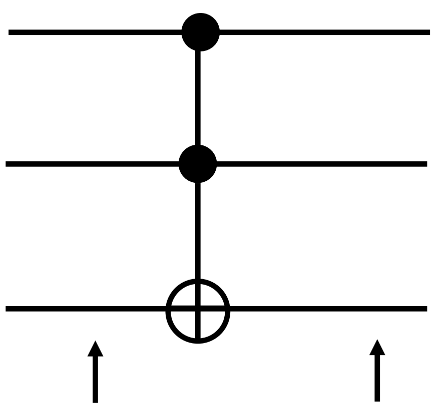
$$U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

S Gate:

$\alpha|0\rangle + \beta|1\rangle$ $\quad \alpha|0\rangle + i\beta|1\rangle$

$$U_S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Toffoli Gate:



$|v\rangle$ $\quad |\psi\rangle$

$$|v\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

In each $|abc\rangle$ Toffoli gate flips *c* if *a* = 1 and *b* = 1. Hence,

$$|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|111\rangle + \alpha_{111}|110\rangle$$

Theorem Classical AND and NOT gates form a universal set, i.e., they allow one to implement any Boolean function.

Let us assume that we have a quantum circuit with input $|v\rangle$ and output $|\psi\rangle$:

We will say that this circuit approximate a unitary operation *U* with error *e* if for all (or almost all) states $|v\rangle$ we have

$$||U|v\rangle - |\psi\rangle||^2 \leq e.$$

Theorem H, S, CNOT, and Toffoli gates form a universal set, in the sense that for any given unitary operator *U* these gates allow one to construct a quantum circuit that approximates *U* with arbitrary small error *e*.

Note that there are many other universal sets of quantum gates.

- For making the approximation error e smaller and smaller, one ,typically, should make the circuit larger and larger (in terms of used quantum gates).

- Let U be a unitary operator that acts on n qubits, that is U is a $2^n\ x\ 2^n$ unitary matrix. Can this U be approximated with small error e and polynomial number of gates, i.e. $O(n^t)$ gates (t is a positive constant)?

- Unfortunately, NOT. There are infinitely many $2^n\ x\ 2^n$ unitary operators U, and for most of them we need exponentially many, i.e., $2^{\alpha n}$ (α is a positive constant), gates.

- Only some "nice" Us can be implemented with small size quantum circuits.

- Good news is that among these nice Us there are unitary transformations that are very useful for solving certain computational problems.

Einstein, Podolsky, Rosen (EPR) pair is a pair of qubits in the state

$$\overset{1\quad 2}{}$$

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

This state happened to be very surprising and useful for many quantum protocols. Note that this is an entangled state (see page 4). Below we consider Quantum Teleportation.

Quantum Teleportation

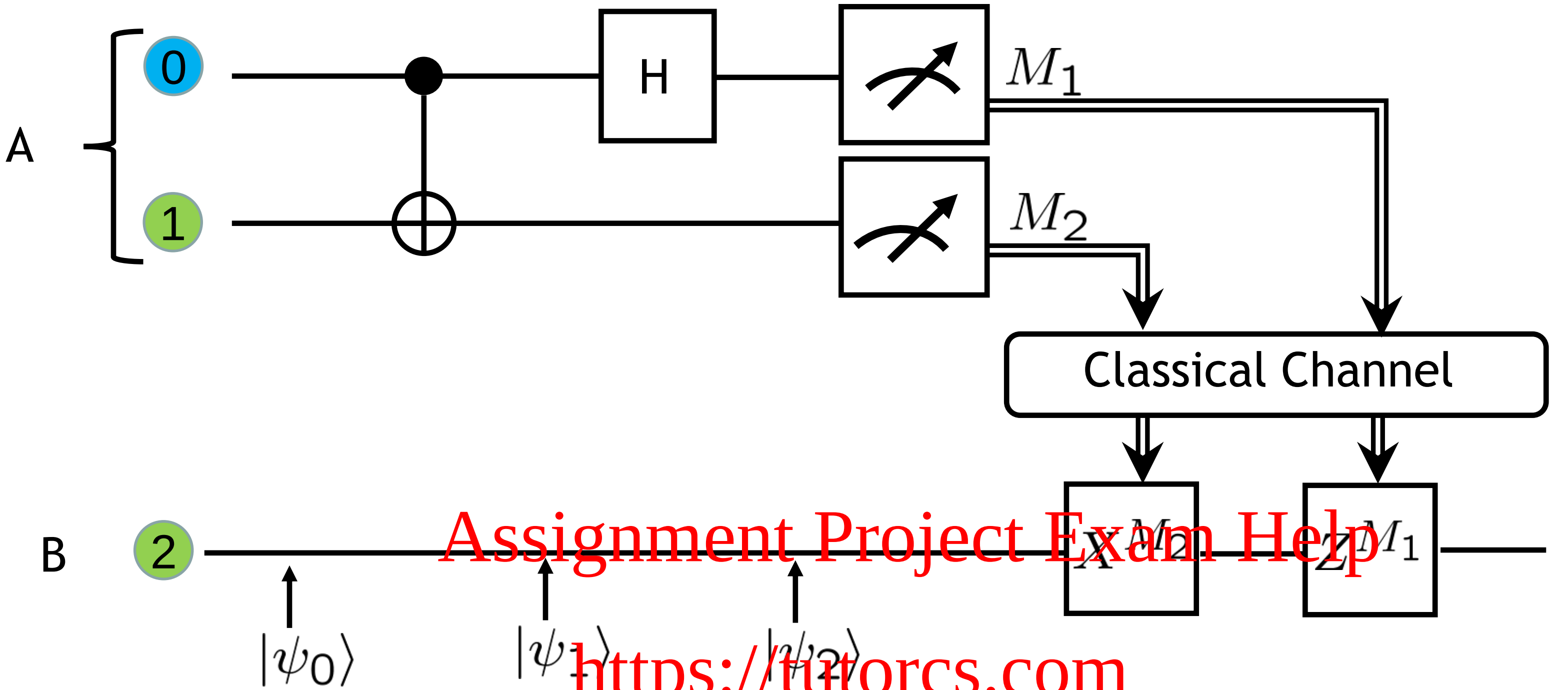
Let us pre-share an EPR pair between Alice (A) and Bob (B). Thus, A has in her possession qubit 1 and Bob has qubit 2

Let A have another qubit 0 in the state $\alpha|1\rangle + \beta|0\rangle$. Alice does not know α and β

Goal: create in Bob's possession a qubit in the state $\alpha|1\rangle + \beta|0\rangle$ using only classical communication; sending qubits to Bob is not allowed.

Actions of Alice: 1. She applies CNOT to qubits 0 and 1; 2. she applies H gate to 0 ; 3. she measures 0 and 1, and sends classical outputs M_1, M_2 to Bob.

On the next page we analyze how the q. state of all 3 qubits evolves during these steps



$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Appling CNOT for 0-th and 1-st qubits, and next factoring out |0> and |1>, we obtain :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$
$$= \frac{\alpha}{\sqrt{2}}|0\rangle(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}|1\rangle(|10\rangle + |01\rangle)$$

After applying H gate to 0-th qubit, making expansion, and factoring out |00>,|01>,|10>, and |11>, we obtain

$$
\begin{aligned}
|\psi_2\rangle &= \frac{\alpha}{2}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \\
&= |00\rangle(\frac{\alpha}{2}|0\rangle + \frac{\beta}{2}|1\rangle) + |01\rangle(\frac{\alpha}{2}|1\rangle + \frac{\beta}{2}|0\rangle) \\
&+ |10\rangle(\frac{\alpha}{2}|0\rangle - \frac{\beta}{2}|1\rangle) + |11\rangle(\frac{\alpha}{2}|1\rangle - \frac{\beta}{2}|0\rangle)
\end{aligned}
$$

Using Measurement Postulate (Postulate 2, page 8) we obtain :

Cl. Output	**Q. Output**	**Probability**
$M_1 = 0, M_2 = 0$	$\|00\rangle(\alpha\|0\rangle + \beta\|1\rangle)$	$1/4$
$M_1 = 0, M_2 = 1$	$\|01\rangle(\alpha\|1\rangle + \beta\|0\rangle)$	$1/4$
$M_1 = 1, M_2 = 0$	$\|10\rangle(\alpha\|0\rangle - \beta\|1\rangle)$	$1/4$
$M_1 = 1, M_2 = 1$	$\|11\rangle(\alpha\|1\rangle - \beta\|0\rangle)$	$1/4$

To get these results you have to apply carefully the measurement postulate to $|\psi_2\rangle$; do not forget about normalization factor γ, which is 2 in this case.

Note that the state of qubit 0 collapsed (either to |0> or |1>).

- Bob gets bits M_1, M_2 and depending on their values he applies a particular unitary operator to qubit 2, as it is shown in the following table.

Values of M_1, M_2	**Bob's Unitary Operator for qubit**
$M_1 = 0, M_2 = 0$	I_4 (meaning do nothing)
$M_1 = 0, M_2 = 1$	X
$M_1 = 1, M_2 = 0$	Z
$M_1 = 1, M_2 = 1$	ZX

here $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- In particular, if $M_1 = 0, M_2 = 0$, then 2 is already in exactly the same state $\alpha|0\rangle + \beta|1\rangle$ as Alice's qubit 0 was originally (see measurement results on the previous page), and so Bob does not have to do anything more

- If $M_1 = 0, M_2 = 1$, then qubit 2 is in the state $\alpha|1\rangle + \beta|0\rangle$, and therefore Bob has to apply *X* to move it to the needed state $\alpha|0\rangle + \beta|1\rangle$
- Cases of other values of M_1, M_2 are similar

Thus, we transferred (teleported) the unknown state $\alpha|0\rangle + \beta|1\rangle$ to Bob without sending any qubit. Amazing!

Quantum teleportation finds many applications. In particular, it is very important for quantum internet and for quantum data exchange inside of a quantum computer.