

Lecture 6

Universal quantum gates

Single qubit + CNOT gates

Single qubit and CNOT gates together can be used to implement an arbitrary two-level unitary operation on the state space of n qubits.

Suppose U is a two-level unitary matrix which acts non-trivially on the space spanned by the computational basis states $|s\rangle$ and $|t\rangle$, where $s = s_1 \dots s_n$ and $t = t_1 \dots t_n$. Let \tilde{U} be non-trivial 2×2 unitary submatrix of U .

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \quad \tilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Goal: to construct a circuit implementing U from single qubit and CNOT gates.

Use Gray codes: A Gray code connecting binary numbers s and t is a sequence of binary numbers, starting with s and concluding with t , such that adjacent members of the list differ in one bit.

Example: $s=101001$, $t=110011$.

Gray code $g_1 \dots g_m$, $g_1 = s$, $g_m = t$:

$$\begin{array}{rcccccc} g_1 & 1 & 0 & 1 & 0 & \textcircled{0} & 1 \\ g_2 & 1 & 0 & \textcircled{1} & 0 & \textcircled{1} & 1 \\ g_3 & 1 & \textcircled{0} & \textcircled{0} & 0 & 1 & 1 \\ g_4 & 1 & \textcircled{1} & 0 & 0 & 1 & 1 \end{array}$$

Basic idea of the quantum circuit implementing U

- Swap the states $|g_1\rangle$ and $|g_2\rangle$.
- Swap the states $|g_2\rangle$ and $|g_3\rangle$ and continue until we swap $|g_{m-2}\rangle$ and $|g_{m-1}\rangle$.
- Apply a controlled- \tilde{U} operation, with the target qubit located at the single bit where g_{m-1} and g_m differ.
- Undo the swap operations: swap $|g_{m-2}\rangle$ and $|g_{m-1}\rangle$, and so on until $|g_2\rangle$ and $|g_1\rangle$ are swapped.

Example: consider the U gate on the previous page.

Question for the class: what logical operation does gate U perform?

U
 $|000\rangle \rightarrow$
 $|001\rangle \rightarrow$
 $|010\rangle \rightarrow$
 $|011\rangle \rightarrow$
 $|100\rangle \rightarrow$
 $|101\rangle \rightarrow$
 $|110\rangle \rightarrow$
 $|111\rangle \rightarrow$

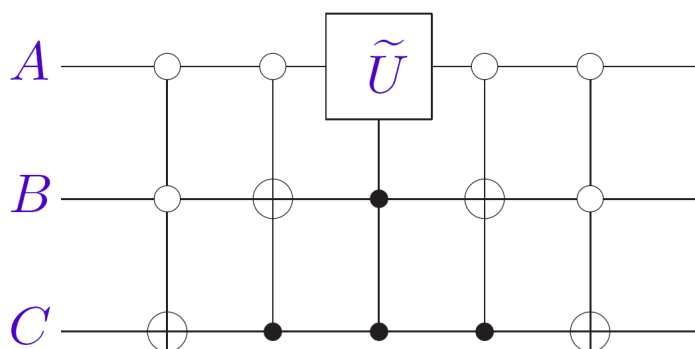


U	
$ 000\rangle$	$\rightarrow a 000\rangle + c 111\rangle$
$ 001\rangle$	$\rightarrow 001\rangle$
$ 010\rangle$	$\rightarrow 010\rangle$
$ 011\rangle$	$\rightarrow 011\rangle$
$ 100\rangle$	$\rightarrow 100\rangle$
$ 101\rangle$	$\rightarrow 101\rangle$
$ 110\rangle$	$\rightarrow 110\rangle$
$ 111\rangle$	$\rightarrow b 000\rangle + d 111\rangle$

Since the U acts non-trivially only on states $|000\rangle$ and $|111\rangle$, the Gray codes is

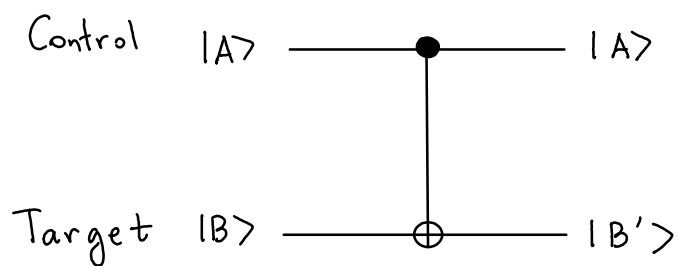
A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

The circuit to implement the gate U is:



REVIEW: Controlled operations: "If A is true, then do B"

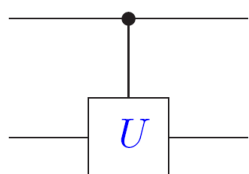
Controlled-NOT (CNOT) gate



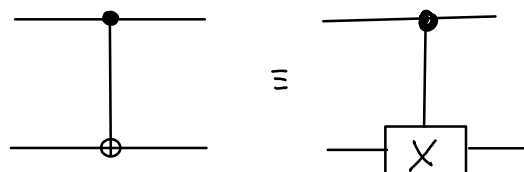
$ AB\rangle$	$ AB'\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

More on controlled operations

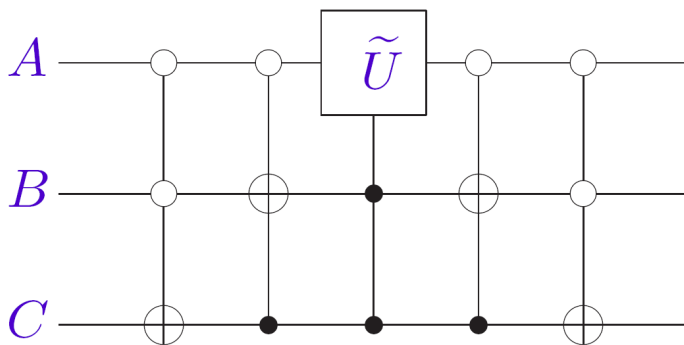
Suppose U is an arbitrary single qubit unitary operation. A controlled- U operation is a two-qubit operation with a control qubit and a target qubit. If control qubit is set, then U is applied to the target qubit.



Example: controlled-NOT gate is controlled-X gate.



The circuit to implement the gate U is:



Class exercise: work out what this circuit does gate by gate.

Hint: you only need to keep track on four states listed in the Gray code as the remaining four states are not affected at all.

ABC	1	2	3
$ 000\rangle$	$ 001\rangle$	$ 011\rangle$	$a 011\rangle + c 111\rangle$
$ 001\rangle$	$ 000\rangle$	$ 000\rangle$	$ 000\rangle$
$ 011\rangle$	$ 011\rangle$	$ 001\rangle$	$ 001\rangle$
$ 111\rangle$	$ 111\rangle$	$ 111\rangle$	$b 011\rangle + d 111\rangle$

\uparrow
 swap $|000\rangle$
 and $|001\rangle$

\uparrow
 swap $|001\rangle$
 and $|011\rangle$

\uparrow
 apply \tilde{U} if both B & A are 11

4	5
$a 001\rangle + c 111\rangle$	$a 000\rangle + c 111\rangle$
$ 000\rangle$	$ 001\rangle$
$ 011\rangle$	$ 011\rangle$
$b 001\rangle + d 111\rangle$	$b 000\rangle + d 111\rangle$

unswap the states back

Measurement

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit.

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not yet measured) at the end of the quantum circuit may be assumed to be measured.

In order for a measurement to be reversible, it must reveal no information about the quantum system being measured!

Summary of the quantum circuit model of computation

- **Classical resources.** For example, many schemes for quantum error-correction involve classical computations to maximize efficiency.
- **A suitable state space.** For a quantum circuit operating on n qubits the state space is 2^n dimensional Hilbert space. Computational basis: $|x_1 \dots x_n\rangle$, where $x_i = 0, 1$.
- **Ability to prepare states in the computational basis.** (Any computational basis state can be prepared in at most n steps.)
- **Ability to perform quantum gates.** The set of Hadamard + phase + CNOT + $\pi/8$ gates is universal.
- **Ability to perform measurements in the computational basis.**

Quantum teleportation

What is it?

Technique for moving quantum states around, even in an absence of quantum communication channel.

The problem:

Alice must deliver qubit $|\psi\rangle$ to Bob

- She does not know the state of the qubit
- She can use only classical channels

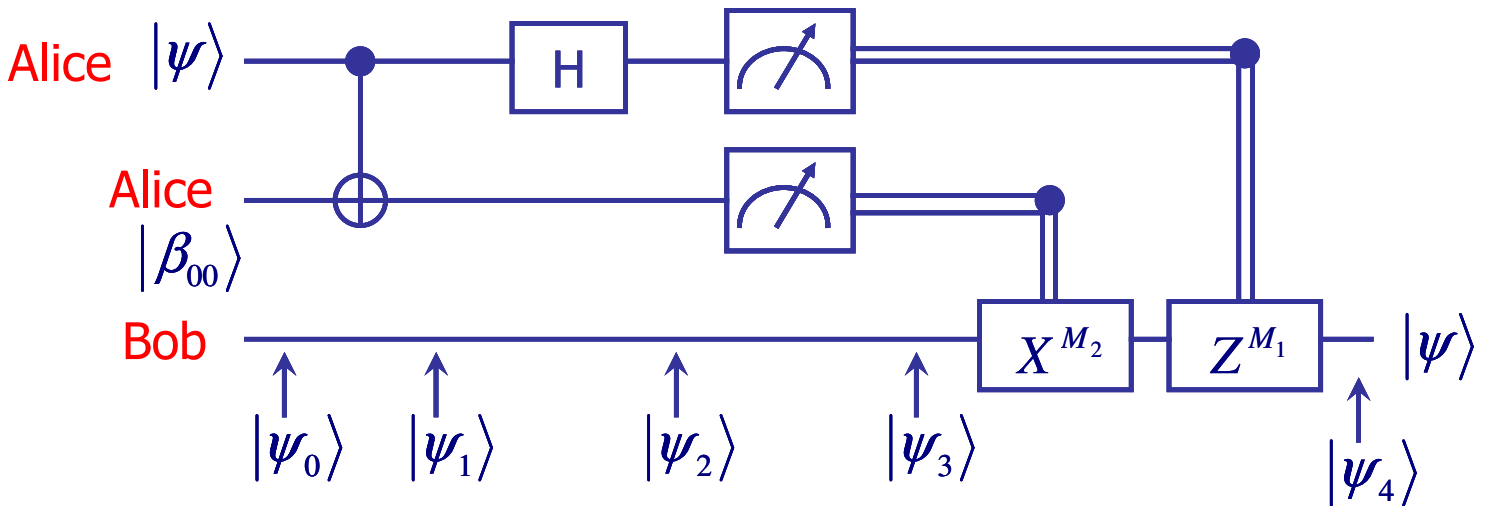
How does it work?

- Alice and Bob generate an EPR pair together.

EPR pair: two entangled qubits in the state $|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

- They moved to different places and each took one qubit of the EPR pair.
- Alice interacts qubit $|\psi\rangle$ to be teleported with half of her EPR pair and then makes a measurement on two qubits which she has.
- She can get one out of four possible results: **00, 01, 10, and 11.**
- Alice reports this information to Bob.
- Bob performs one of four operations on his half of the EPR pair.
- Amazingly, he can recover the original state $|\psi\rangle$!

Teleportation scheme

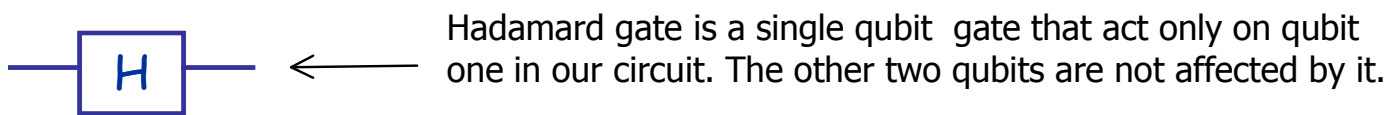


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

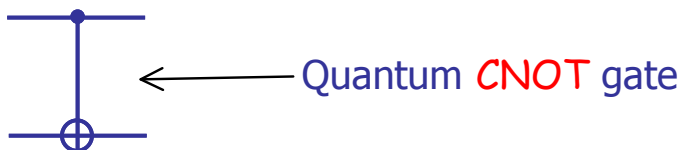
Quantum circuit

1. Each line represents one qubit.
Therefore, we have three qubits in our teleportation circuit.

2. If the gate is on a single line, this is a one-qubit gate applied to this one qubit only.



3. If two lines are connected, it signifies the two qubit gate that acts of these two qubits only.



4. Measurement is designated by sign 

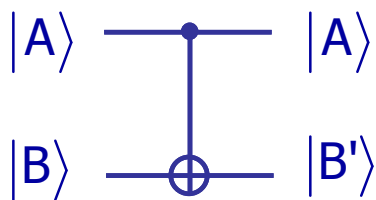
We will now work out in detail how this circuit works.

The initial state is

$$\begin{aligned}
 |\psi_0\rangle &= |\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle) \right] \\
 &= \frac{1}{\sqrt{2}} \left[\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle \right]
 \end{aligned}$$

Next, we find the state $|\psi_1\rangle$.

The CNOT gate (control-NOT) works in the following way:



$ AB\rangle$	$ AB'\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

Logical operation: if A is in state $|1\rangle$, flip the qubit B.

Class exercise: what is $|\psi_1\rangle$?

$$\begin{aligned}
 |\psi_0\rangle &= \frac{1}{\sqrt{2}} \left[\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle \right] \\
 |\psi_1\rangle &= \frac{1}{\sqrt{2}} \left[\alpha |000\rangle + \alpha |011\rangle + \beta |110\rangle + \beta |101\rangle \right]
 \end{aligned}$$

The next step involves Hadamard gate . First, we need to find out what Hadamard gate does to a qubit. The matrix for the Hadamard gate is

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

Class exercise: If you operate by this gate on some unknown qubit, what will you get?

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{H} ?$$

Hint: you need to work out $H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \dots$

$$\begin{aligned} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \left(\alpha \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{|0\rangle} + \beta \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{|1\rangle} + \alpha \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{|1\rangle} - \beta \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{|0\rangle} \right) \\ &= \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

Another way to do it is to find how H acts on $|0\rangle$ and $|1\rangle$:

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

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Result:

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{H}} \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Therefore, the Hadamard gate corresponds to the following logical operation:

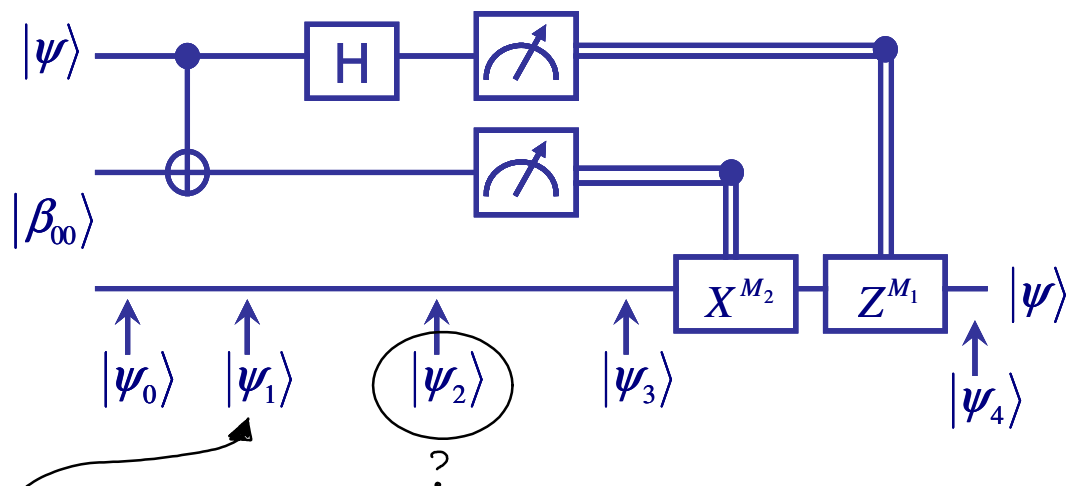
If the qubit is in state $|0\rangle$ it will become $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$.

If the qubit is in state $|1\rangle$ it will become $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Now we can work out the next step of our circuit.

Class exercise: what is $|\psi_2\rangle$? In your result, separate out the last third qubit and group together terms with the same states for the first two qubits, i.e. your result should be written as

$$|\psi_2\rangle = \frac{1}{2} \{ |00\rangle (\quad) + |01\rangle (\quad) + |10\rangle (\quad) + |11\rangle (\quad) \}.$$



$$|\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha |000\rangle + \alpha |011\rangle + \beta |110\rangle + \beta |101\rangle]$$

$$\begin{aligned}
 & |0\rangle \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
 \text{H:} & \\
 & |1\rangle \longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}
 \end{aligned}$$

$$\begin{aligned}
 |\Psi_2\rangle &= \frac{1}{\sqrt{2}} \left\{ \alpha H|0\rangle|00\rangle + \alpha H|0\rangle|11\rangle + \beta H|1\rangle|10\rangle + \beta H|1\rangle|01\rangle \right\} \\
 &= \frac{1}{2} \left\{ \alpha(|0\rangle + |1\rangle)|00\rangle + \alpha(|0\rangle + |1\rangle)|11\rangle + \beta(|0\rangle - |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|01\rangle \right\} \\
 &= \frac{1}{2} \left\{ \alpha|100\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle \right. \\
 &\quad \left. + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle \right\} \\
 &= \frac{1}{2} \left\{ \alpha|00\rangle|0\rangle + \alpha|10\rangle|0\rangle + \alpha|01\rangle|1\rangle + \alpha|11\rangle|1\rangle \right. \\
 &\quad \left. + \beta|01\rangle|0\rangle - \beta|11\rangle|0\rangle + \beta|00\rangle|1\rangle - \beta|10\rangle|1\rangle \right\} \\
 &= \frac{1}{2} \left\{ |00\rangle (\alpha|0\rangle + \beta|1\rangle) \right. \\
 &\quad + |01\rangle (\alpha|1\rangle + \beta|0\rangle) \\
 &\quad + |10\rangle (\alpha|0\rangle - \beta|1\rangle) \\
 &\quad \left. + |11\rangle (\alpha|1\rangle - \beta|0\rangle) \right\}
 \end{aligned}$$

$$|\psi_2\rangle = \frac{1}{2} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

Next step: measure the state of first two qubit. Possible results are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. After Alice makes the measurement, she communicates the result to Bob. Bob does the following conditional operation with his qubit:

- 1) If result is $|00\rangle$, he does nothing: he already has the qubit $|\psi\rangle$!
- 2) If result is $|01\rangle$, he applies X gate.
- 3) If result is $|10\rangle$, he applies Z gate.
- 4) If result is $|11\rangle$, he applies both X and Z gate.

$$\alpha|0\rangle + \beta|1\rangle \text{ --- } \boxed{X} \text{ --- } \alpha|1\rangle + \beta|0\rangle$$

$$|01\rangle \Rightarrow X(\alpha|1\rangle + \beta|0\rangle) \rightarrow \alpha|0\rangle + \beta|1\rangle \equiv |\psi\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \text{ --- } \boxed{Z} \text{ --- } \alpha|0\rangle - \beta|1\rangle$$

$$|10\rangle \Rightarrow Z(\alpha|0\rangle - \beta|1\rangle) \rightarrow \alpha|0\rangle + \beta|1\rangle \equiv |\psi\rangle$$

$$|11\rangle \Rightarrow XZ(\alpha|1\rangle - \beta|0\rangle) \rightarrow \alpha|0\rangle + \beta|1\rangle \equiv |\psi\rangle$$