

Department of Information Engineering
MSc in Computer Engineering (a.y. 2024/2025)
University of Pisa

*Quantum Computing
and
Quantum Internet*

Luciano Lenzini
Full Professor
Department of Information Engineering
School of Engineering
University of Pisa, Italy
e-mail: lenzini44@gmail.com
<http://www.iet.unipi.it/~lenzini/>
<http://www.originiinternetitalia.it/it/>



A Quantum Model of Computation

The Quantum Circuit Model

- We've already met a few simple quantum circuits
- Let's look in a little more detail at the elements of a quantum circuit
- A simple quantum circuit containing three quantum gates has already been discussed
- The output of the third gate (Z) is a qubit in state $ZSH|0\rangle$



The Quantum Circuit Model

- Each line in the circuit represents a *wire* in the quantum circuit
- This wire does not necessarily correspond to a **physical wire**; it may correspond instead to a physical particle such as a photon moving from one location to another through space
- It is conventional to assume that the state input to the circuit is a computational basis state, *usually* the state consisting of $|0\rangle_s$

However, other input states, such as $|+\rangle, |-\rangle$, are possible

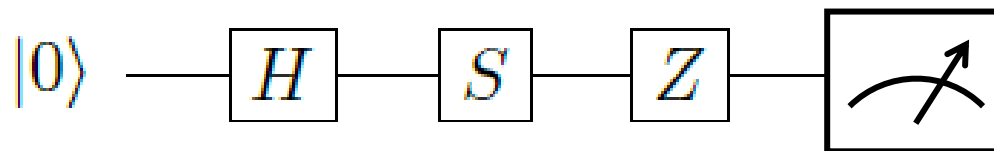


Combination of Quantum Gates

- The circuit is read **left-to-right**, just like a classical circuit diagram
- So, we start with a single qubit in the $|0\rangle$ state and apply a Hadamard gate H to it, followed by a phase gate S , and finally a Z gate

$$ZSH|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{\sqrt{2}} [|0\rangle - i|1\rangle]$$

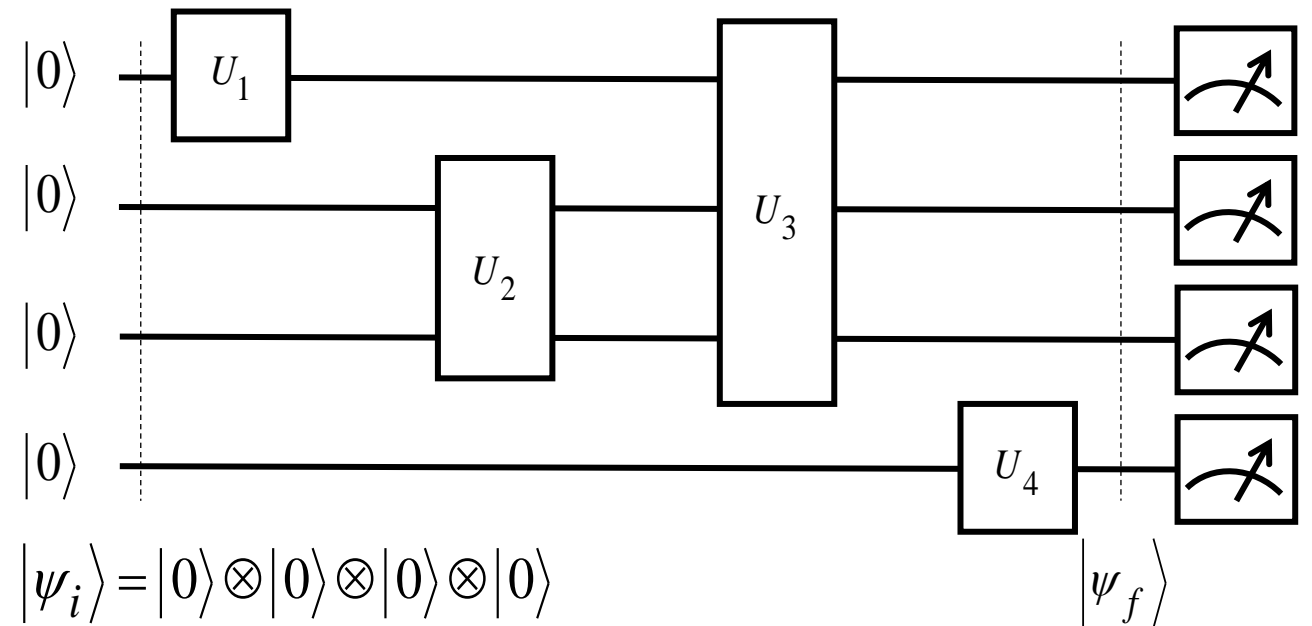
and if we *measure* the qubit we get $|0\rangle$ or $|1\rangle$ with equal probability



The Quantum Circuit Model

As we proceed, we'll introduce new quantum gates as needed.

The previous quantum circuit model can be extended to quantum circuit models that are capable of transforming the state of two qubits or more.



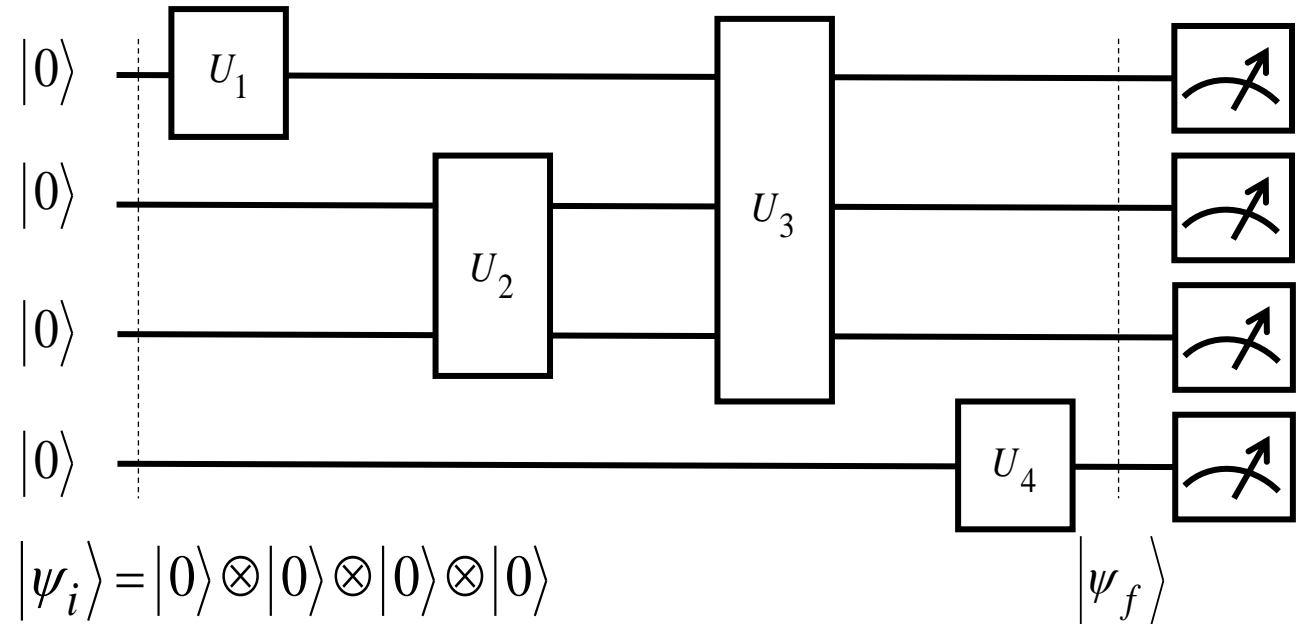
The Quantum Circuit Model

The four-qubit state

$$|\psi_i\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$$

enters the circuit at the left.

These qubits are processed by the gates U_1 , U_2 , U_3 , and U_4 .

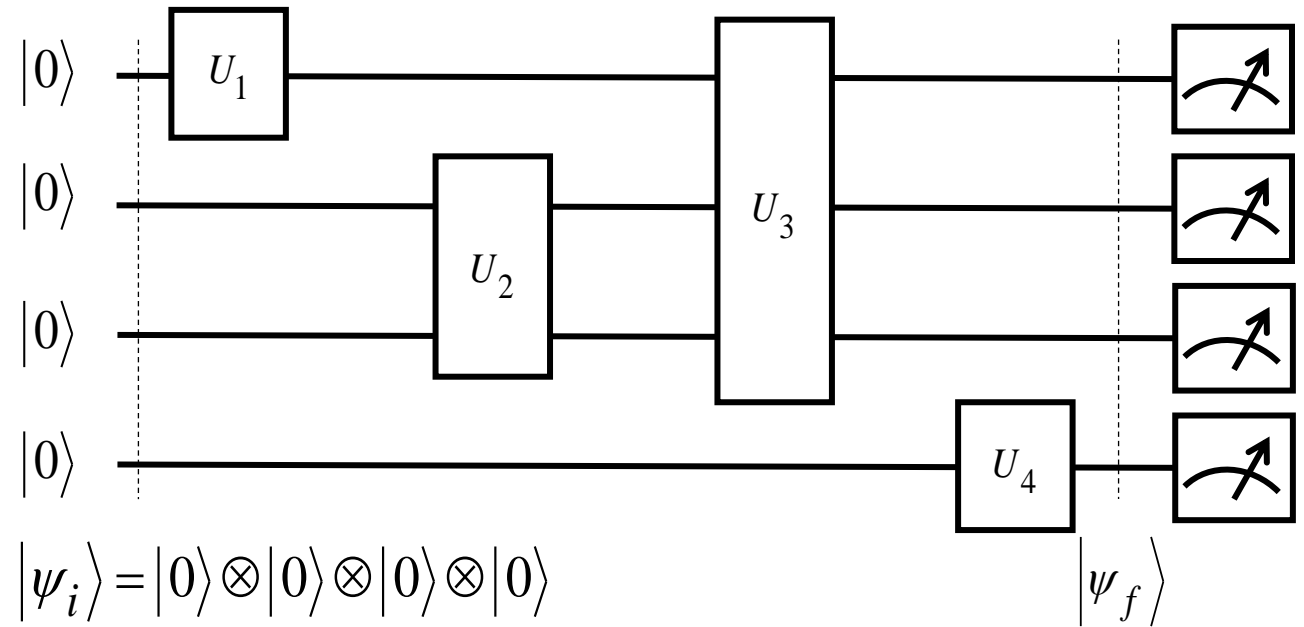


At the output of the circuit, we have the collective 4-qubit state $|\psi_f\rangle$

The Quantum Circuit Model

A measurement is then made of the resulting state

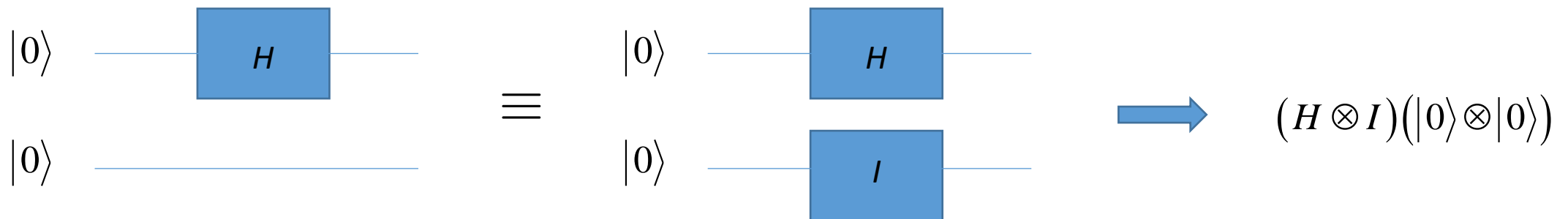
The measurement will often be a simple qubit-by-qubit measurement in the CBS basis, but in some cases may be a more general measurement of the joint state.



In the following, we take a closer look at the two-qubit gates

Two-Qubit Quantum Gates

- Assume we have multiple qubits, and we want to apply a single-qubit gate (like I , X , Y , Z , S , T , or H) to just a single qubit
- For example, say we have two qubits in the $|00\rangle = |0\rangle \otimes |0\rangle$ state, and we want to apply the Hadamard gate to the left qubit, but leave the right qubit alone (i.e., apply the **identity** gate to it)
- We write the gates using a tensor product, so we write

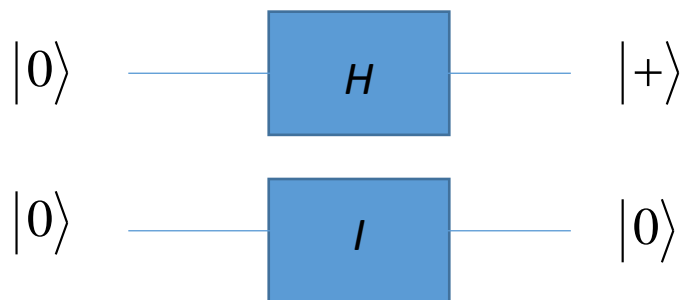


Two-Qubit Quantum Gates

$$\begin{aligned}
 (H \otimes I)(|0\rangle \otimes |0\rangle) &= H|0\rangle \otimes I|0\rangle = |+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\
 &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}
 \end{aligned}$$

$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$



$$(H \otimes I)(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Two-Qubit Quantum Gates

- We can find $H \otimes I$ as a matrix in two different ways
- *First*, we can find how $H \otimes I$ acts on each of the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- We already found how it acts on $|00\rangle$. We just carry on with the rest.

$$(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$(H \otimes I)|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$(H \otimes I)|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$$

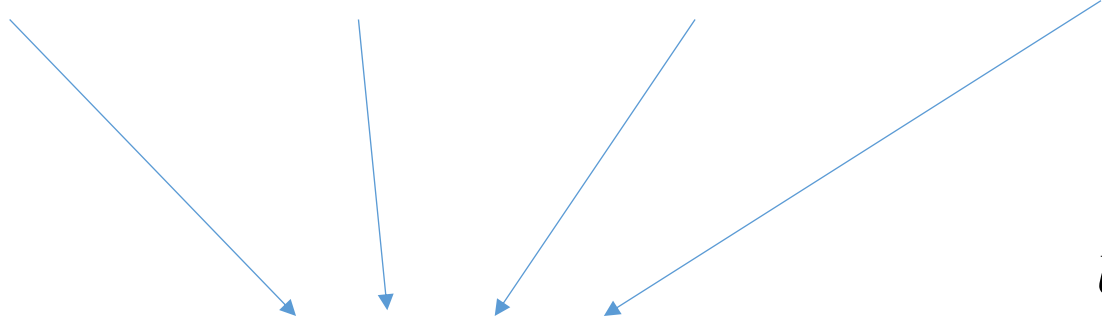
$$(H \otimes I)|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix}$$

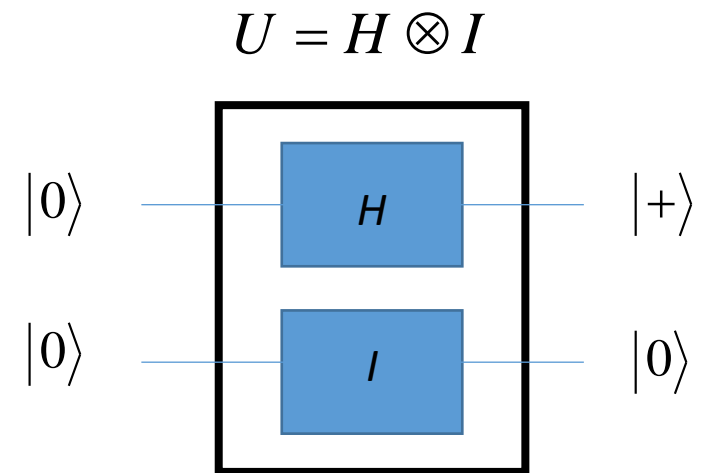
Two-Qubit Quantum Gates

- We can write $H \otimes I$ as a matrix by combining the column vectors for

$$H \otimes I \equiv \left[(H \otimes I)|00\rangle, (H \otimes I)|01\rangle, (H \otimes I)|10\rangle, (H \otimes I)|11\rangle \right]$$

as a 4x4 grid:


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



Two-Qubit Quantum Gates

- The *second way* to find this matrix is by taking the Kronecker product of H and X :

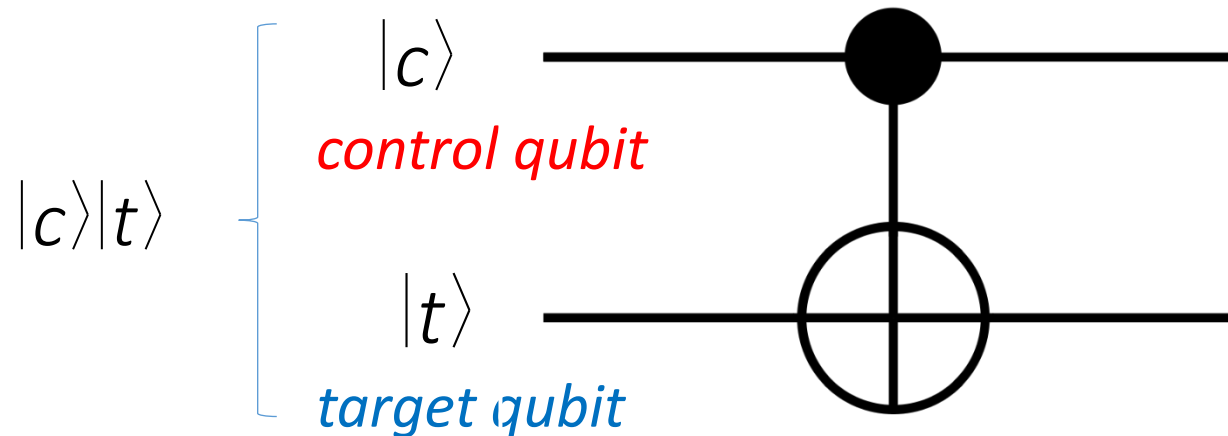
$$\begin{aligned} H \otimes I &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & -1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \end{aligned}$$

Two-Qubit Quantum Gates

- Quantum gates can also operate on two qubits at the same time
- Some important examples include:
 1. The *CNOT gate* or *controlled-NOT gate*, or since the X gate is the *NOT* gate, the *CNOT gate* is also called the *cX gate* or *controlled-X gate*
 2. The controlled- U gate
 3. The *SWAP* gate

CNOT Gate

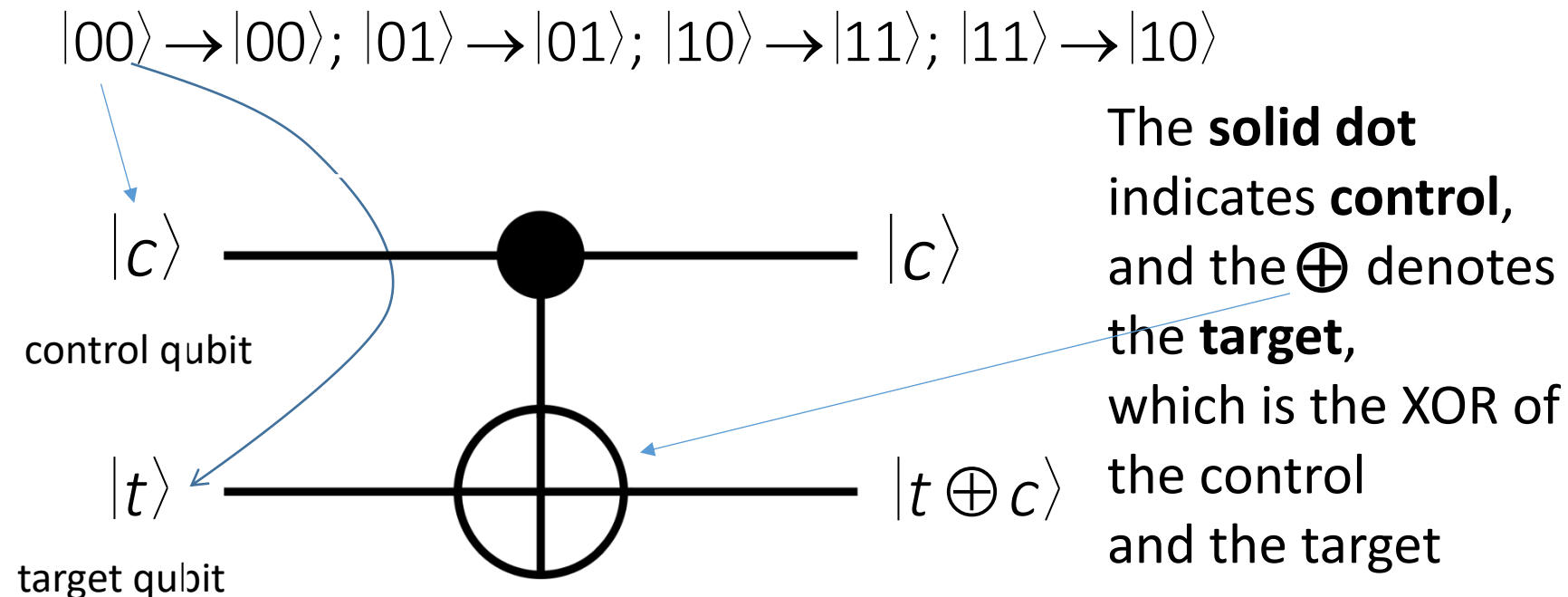
- This is the simplest and most commonly used *2-qubit gate* in quantum computing
- The *controlled-NOT* or CNOT gate has two input qubits, known as the *control qubit* (top line) and the *target qubit* (bottom line), respectively



CNOT Gate

The action of the gate

- If the *control qubit* is set to $|0\rangle$, then *nothing happens to the target qubit*
- If the *control qubit* is set to $|1\rangle$, then *the target qubit is flipped*



XOR gate truth table

Input		Output
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

CNOT Gate

- Formally

$$CNOT|00\rangle = |00\rangle$$

$$CNOT|01\rangle = |01\rangle$$

$$CNOT|10\rangle = |11\rangle$$

$$CNOT|11\rangle = |10\rangle$$

$$\rightarrow CNOT|c\rangle|t\rangle = |c\rangle|c \oplus t\rangle, \quad \forall c, t \in \{0, 1\}$$

The amplitudes of $|10\rangle$ and $|11\rangle$ are swapped

- In vectorial form

$$CNOT|00\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$CNOT|01\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$CNOT|10\rangle = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$CNOT|11\rangle = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

CNOT Gate

- Acting on a superposition,

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

$$\begin{aligned} \text{CNOT}|\psi\rangle &= \text{CNOT}(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle) \\ &= c_0\text{CNOT}|00\rangle + c_1\text{CNOT}|01\rangle + c_2\text{CNOT}|10\rangle + c_3\text{CNOT}|11\rangle \\ &= c_0|00\rangle + c_1|01\rangle + c_2|11\rangle + c_3|10\rangle \\ &= c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle \end{aligned}$$

CNOT Gate

- Let's now consider the following expression:

$$\text{CNOT}|\psi\rangle = c_0\text{CNOT}|00\rangle + c_1\text{CNOT}|01\rangle + c_2\text{CNOT}|10\rangle + c_3\text{CNOT}|11\rangle$$

that can be written, in matrix form, as follows:

$$\text{CNOT}|\psi\rangle = \begin{bmatrix} \text{CNOT}|00\rangle & \text{CNOT}|01\rangle & \text{CNOT}|10\rangle & \text{CNOT}|11\rangle \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{bmatrix}$$

CNOT Gate

- Thus, in the computational basis

$$\{|\text{control,target}\rangle\} \equiv \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

the matrix representation of CNOT is

$$CNOT = \begin{bmatrix} CNOT|00\rangle & CNOT|01\rangle & CNOT|10\rangle & CNOT|11\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

CNOT Gate

- Applying CNOT to the general state

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

we get

$$CNOT|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{bmatrix} = c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle$$

CNOT Gate

- Since

$$CNOT = CNOT^\dagger$$

and because

$$CNOT \cdot CNOT^\dagger = CNOT^\dagger \cdot CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

it follows

$$CNOT^2 = I$$

CNOT Gate

- We can express *CNOT* by means of *outer products*

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

CNOT Gate

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$$

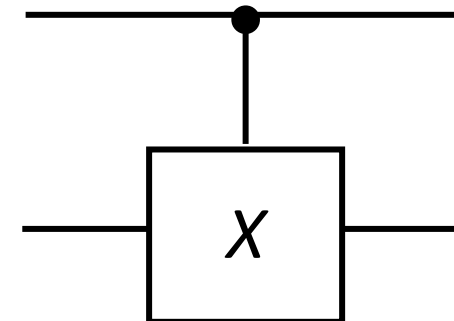
$$\begin{aligned} |00\rangle\langle 00| &= (|0\rangle_A \otimes |0\rangle_B)(\langle 0|_A \otimes \langle 0|_B) = (|0\rangle_A \langle 0|) \otimes (|0\rangle_B \langle 0|) & |10\rangle\langle 11| &= (|1\rangle_A \otimes |0\rangle_B)(\langle 1|_A \otimes \langle 1|_B) = (|1\rangle_A \langle 1|) \otimes (|0\rangle_B \langle 1|) \\ |01\rangle\langle 01| &= (|0\rangle_A \otimes |1\rangle_B)(\langle 0|_A \otimes \langle 1|_B) = (|0\rangle_A \langle 0|) \otimes (|1\rangle_B \langle 1|) & |11\rangle\langle 10| &= (|1\rangle_A \otimes |1\rangle_B)(\langle 1|_A \otimes \langle 0|_B) = (|1\rangle_A \langle 1|) \otimes (|1\rangle_B \langle 0|) \end{aligned}$$

- By exploiting the previous results

$$\begin{aligned} CNOT &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \\ &= (|0\rangle_A \langle 0|) \otimes (|0\rangle_B \langle 0|) + (|0\rangle_A \langle 0|) \otimes (|1\rangle_B \langle 1|) + (|1\rangle_A \langle 1|) \otimes (|0\rangle_B \langle 1|) + (|1\rangle_A \langle 1|) \otimes (|1\rangle_B \langle 0|) \\ &= |0\rangle_A \langle 0| \otimes (|0\rangle_B \langle 0| + |1\rangle_B \langle 1|) + |1\rangle_A \langle 1| \otimes (|0\rangle_B \langle 1| + |1\rangle_B \langle 0|) \\ &= |0\rangle_A \langle 0| \otimes I_B + |1\rangle_A \langle 1| \otimes X_B \end{aligned}$$



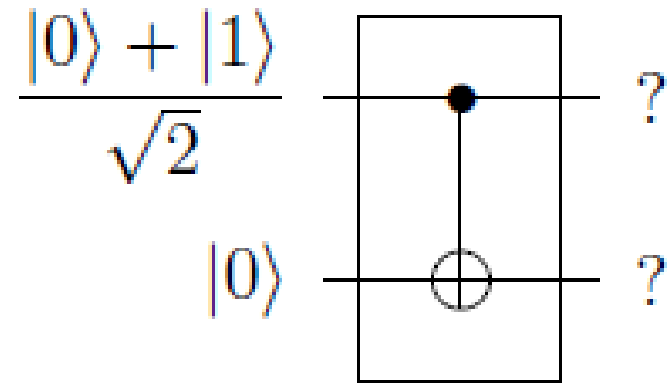
$$CNOT = |0\rangle_A \langle 0| \otimes I_B + |1\rangle_A \langle 1| \otimes X_B$$



Quantum Entanglement for CNOT

- A separable bipartite state into CNOT gate *does not usually result* in a *separable state* out of CNOT
- To see this, consider the separable state

$$|\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle)$$

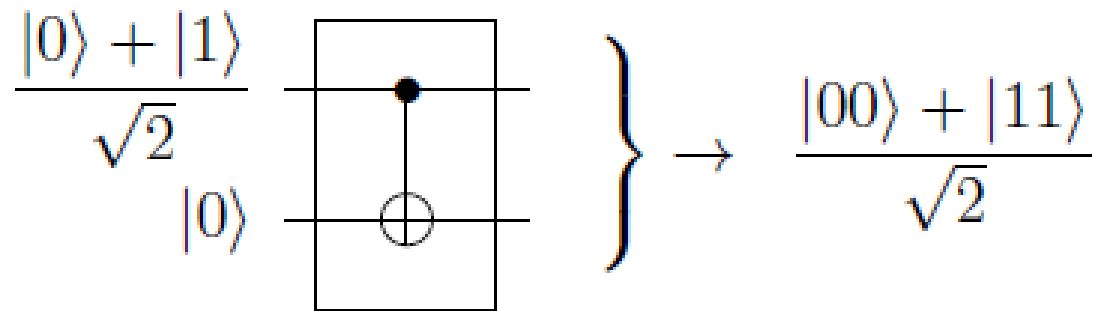


Quantum Entanglement for CNOT

- Now, apply CNOT using linearity,

$$CNOT|\psi\rangle = \frac{1}{\sqrt{2}}(CNOT|00\rangle + CNOT|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- This is the true output of the gate for the presented input
- The output state is not separable



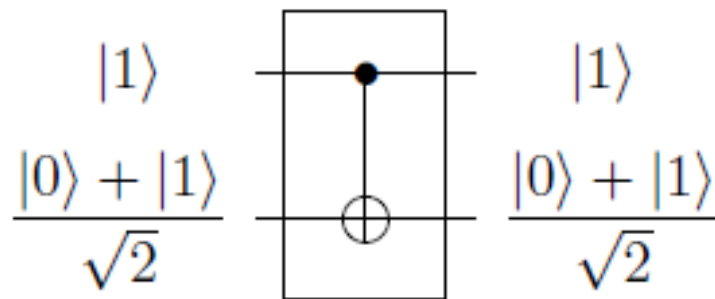
Quantum Entanglement for CNOT

- Now, consider the separable state

$$|\psi\rangle = |1\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle)$$

and apply CNOT

$$CNOT|\psi\rangle = \frac{1}{\sqrt{2}} (CNOT|10\rangle + CNOT|11\rangle) = \frac{1}{\sqrt{2}} (|11\rangle + |10\rangle) = |1\rangle \left(\frac{|1\rangle + |0\rangle}{\sqrt{2}} \right)$$



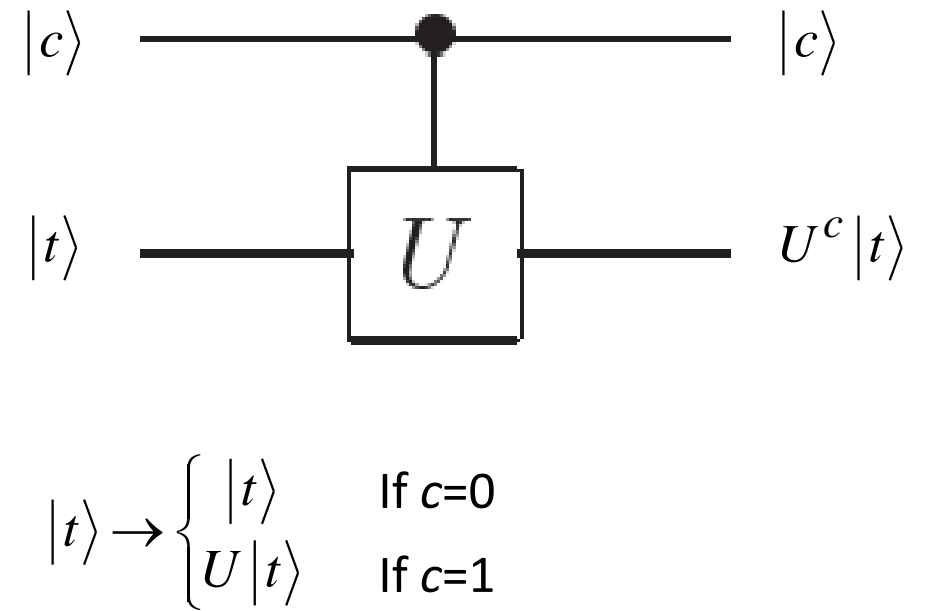
Aha! *separable*. That's because the control-bit is a basis element; it does not change during the linear application of CNOT so will be conveniently available for CNOT factoring at the output

CNOT on the X Basis

Initial state in Hadamard basis	Equivalent state in computational basis	Apply operator	State in computational basis after C_{NOT}	Equivalent state in Hadamard basis
$ ++\rangle$	$\frac{1}{2}(00\rangle + 01\rangle + 10\rangle + 11\rangle)$	C_{NOT}	$\frac{1}{2}(00\rangle + 01\rangle + 11\rangle + 10\rangle)$	$ ++\rangle$
$ +-\rangle$	$\frac{1}{2}(00\rangle - 01\rangle + 10\rangle - 11\rangle)$	C_{NOT}	$\frac{1}{2}(00\rangle - 01\rangle + 11\rangle - 10\rangle)$	$ --\rangle$
$ -+\rangle$	$\frac{1}{2}(00\rangle + 01\rangle - 10\rangle - 11\rangle)$	C_{NOT}	$\frac{1}{2}(00\rangle + 01\rangle - 11\rangle - 10\rangle)$	$ -+\rangle$
$ --\rangle$	$\frac{1}{2}(00\rangle - 01\rangle - 10\rangle + 11\rangle)$	C_{NOT}	$\frac{1}{2}(00\rangle - 01\rangle - 11\rangle + 10\rangle)$	$ +-\rangle$

The *controlled-U* Gate

- Suppose U is an arbitrary single qubit unitary operation
- A *controlled-U* (CU) operation is a two-qubit operation, again with a control and a target qubit
- If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone; that is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c |t\rangle$



The *controlled-U* Gate

- Formally

$$CU|00\rangle = |00\rangle$$

$$CU|01\rangle = |01\rangle$$

$$CU|10\rangle = |1\rangle \otimes U|0\rangle$$

$$CU|11\rangle = |1\rangle \otimes U|1\rangle$$

- To get the matrix representation of CU , first say U acts on a single qubit as

$$U|0\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} U_{00} \\ U_{10} \end{bmatrix} = U_{00}|0\rangle + U_{10}|1\rangle$$


$$U|1\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} U_{01} \\ U_{11} \end{bmatrix} = U_{01}|0\rangle + U_{11}|1\rangle$$

The *controlled-U* Gate

- Thus

$$CU|10\rangle = |1\rangle \otimes U|0\rangle = |1\rangle \otimes (U_{00}|0\rangle + U_{10}|1\rangle) = U_{00}|10\rangle + U_{10}|11\rangle$$

$$CU|11\rangle = |1\rangle \otimes U|1\rangle = |1\rangle \otimes (U_{01}|0\rangle + U_{11}|1\rangle) = U_{01}|10\rangle + U_{11}|11\rangle$$


$$U|0\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} U_{00} \\ U_{10} \end{bmatrix} = U_{00}|0\rangle + U_{10}|1\rangle$$
$$U|1\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} U_{01} \\ U_{11} \end{bmatrix} = U_{01}|0\rangle + U_{11}|1\rangle$$

- Since

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

To help understand the algebraic passages, I show the results obtained in the previous slide.

The *controlled-U* gate

- It follows

$$CU|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad CU|01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad CU|10\rangle = \begin{bmatrix} 0 \\ 0 \\ U_{00} \\ U_{10} \end{bmatrix} \quad CU|11\rangle = \begin{bmatrix} 0 \\ 0 \\ U_{01} \\ U_{11} \end{bmatrix}$$

- Thus, in the computational basis the matrix representation of CU is

$$CU = [CU|00\rangle \quad CU|01\rangle \quad CU|10\rangle \quad CU|11\rangle] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix}$$

The *controlled-U* gate

Behavior on general state

$$\begin{aligned} |\psi\rangle &= \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \quad \longrightarrow \quad CU|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ U_{00}\gamma + U_{01}\delta \\ U_{10}\gamma + U_{11}\delta \end{bmatrix} \\ &= \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + (U_{00}\gamma + U_{01}\delta)|1\rangle|0\rangle + (U_{10}\gamma + U_{11}\delta)|1\rangle|1\rangle \end{aligned}$$

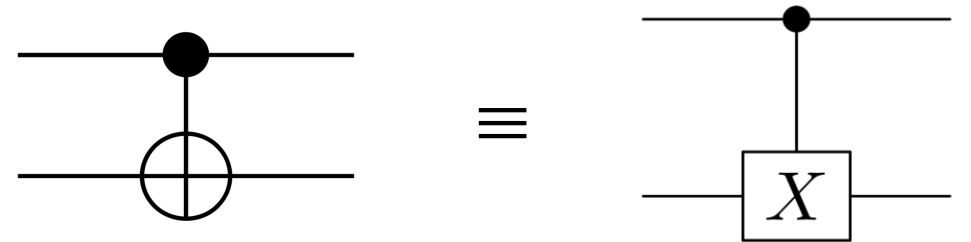
The *controlled-X* Gate

- Let's focus on the *controlled-X* gate
- In this case $U=X$

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{matrix} U_{00} = U_{11} = 0 \\ U_{01} = U_{10} = 1 \end{matrix} \quad \longrightarrow \quad CU = CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \text{CNOT}$$

CX can also be written as

$$CX = CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$



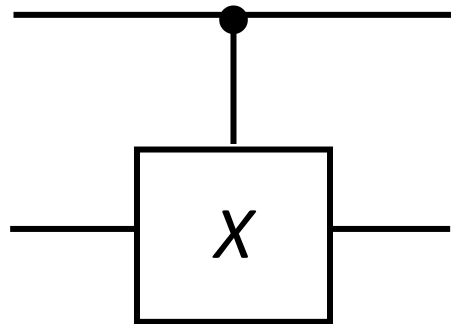
The *controlled-X* Gate

Behavior on general state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$



$$CX|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{bmatrix}$$



$$= \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \delta|1\rangle|0\rangle + \gamma|1\rangle|1\rangle$$

The *controlled-Z* Gate

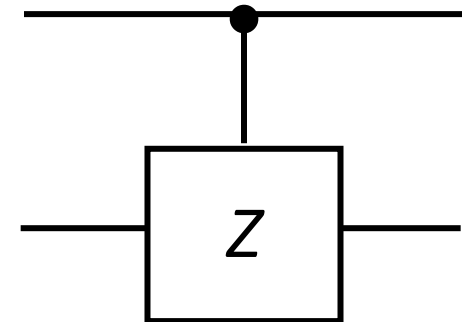
- Let's consider the *controlled-Z* gate
- In this case $U=Z$

$$U = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{array}{l} U_{00} = 1 \\ U_{11} = -1 \\ U_{01} = U_{10} = 0 \end{array} \quad \longrightarrow$$

$$CU = CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

CZ can also be written as

$$CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$$

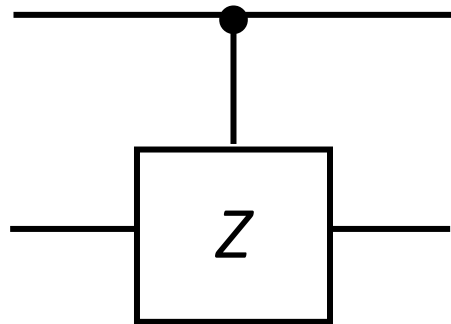


The *controlled*-Z Gate

Behavior on general state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \quad \rightarrow$$

$$CZ|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ -\delta \end{bmatrix}$$



$$= \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle - \delta|1\rangle|1\rangle$$

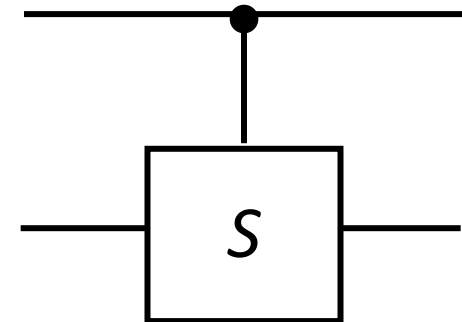
The *controlled-S* Gate

- Let's consider the controlled-S gate
- In this case $U=S$

$$U = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad \begin{matrix} U_{00} = 1 \\ U_{11} = i \\ U_{01} = U_{10} = 0 \end{matrix} \quad \longrightarrow \quad CU = CS = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

CS can also be written as

$$CS = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + i|11\rangle\langle 11|$$



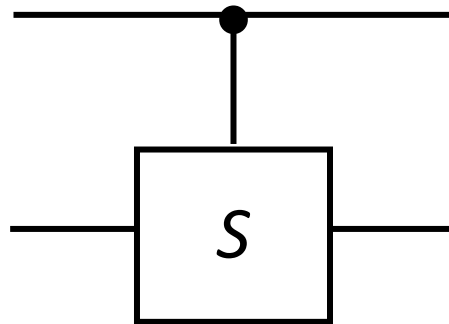
The *controlled-S* Gate

Behavior on general state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$



$$CS|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ i\delta \end{bmatrix}$$



$$= \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + i\delta|1\rangle|1\rangle$$

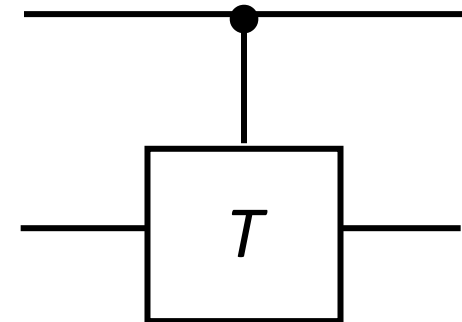
The *controlled-T* Gate

- Let's consider the controlled- T gate
- In this case $U=T$

$$U = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{array}{l} U_{00} = 1 \\ U_{11} = e^{i\pi/4} \\ U_{01} = U_{10} = 0 \end{array} \longrightarrow CU = CT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix}$$

CT can also be written as

$$CT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\pi/4} |11\rangle\langle 11|$$



The *controlled-T* Gate

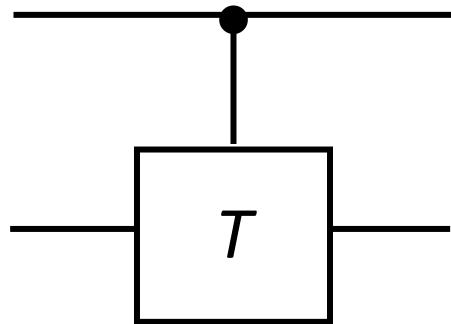
Behavior on general state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$



$$CT|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ e^{i\pi/4}\delta \end{bmatrix}$$

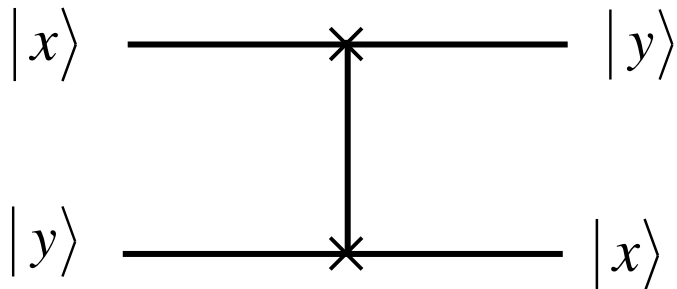
$$= \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + e^{i\pi/4}\delta|1\rangle|1\rangle$$



The *SWAP* Gate

- The *SWAP* gate is two-qubit operation
- Expressed in computational basis, the *SWAP* gate swaps the state of the two qubits involved in the operation

$$\begin{aligned} \text{SWAP}|00\rangle &= |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} & \text{SWAP}|01\rangle &= |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} & \text{SWAP}|10\rangle &= |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} & \text{SWAP}|11\rangle &= |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned}$$



In other words, $\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$ for $x, y \in \{0, 1\}$

The *SWAP* Gate

- Thus, in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ the matrix representation of SWAP is

$$SWAP = \begin{bmatrix} SWAP|00\rangle & SWAP|01\rangle & SWAP|10\rangle & SWAP|11\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- *SWAP* can also be written as

$$SWAP = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

The *SWAP* Gate

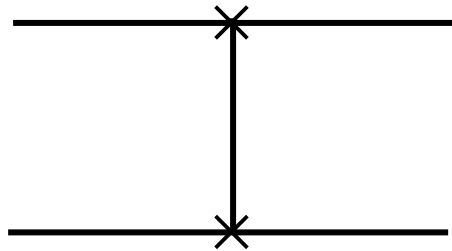
Behavior on general state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$



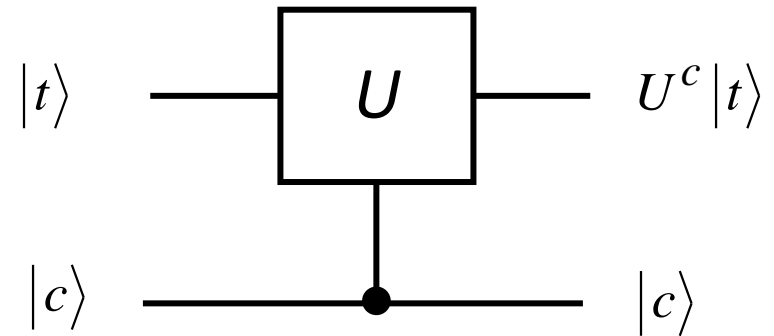
$$SWAP|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{bmatrix}$$

$$= \alpha|0\rangle|0\rangle + \gamma|0\rangle|1\rangle + \beta|1\rangle|0\rangle + \delta|1\rangle|1\rangle$$



Swapping Roles in *controlled-U* Gate

- We could have (and still can) turn any of our controlled gates upside down
- Let's refer to this version of a controlled gate using the notation $(C \uparrow)U$
- It is easy to derive the matrix on the standard basis



$$|t\rangle \rightarrow \begin{cases} |t\rangle & \text{If } c=0 \\ U|t\rangle & \text{If } c=1 \end{cases}$$

Swapping Roles in *controlled-U* Gate

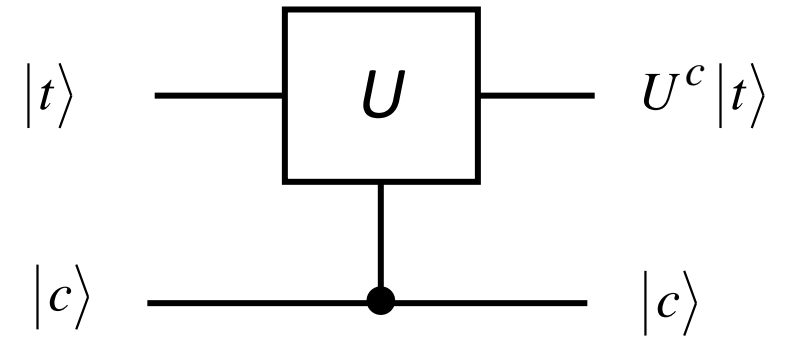
- Before continuing, take into account the results listed below

$$U|0\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} U_{00} \\ U_{10} \end{bmatrix} = U_{00}|0\rangle + U_{10}|1\rangle$$

$$\longrightarrow U|0\rangle = U_{00}|0\rangle + U_{10}|1\rangle$$

$$U|1\rangle = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} U_{01} \\ U_{11} \end{bmatrix} = U_{01}|0\rangle + U_{11}|1\rangle$$

$$\longrightarrow U|1\rangle = U_{01}|0\rangle + U_{11}|1\rangle$$



$$|t\rangle \rightarrow \begin{cases} |t\rangle & \text{If } c=0 \\ U|t\rangle & \text{If } c=1 \end{cases}$$

Swapping Roles in *controlled-U* Gate

- Thus

$$(c \uparrow)U|00\rangle = |00\rangle$$

$$(c \uparrow)U|10\rangle = |10\rangle$$

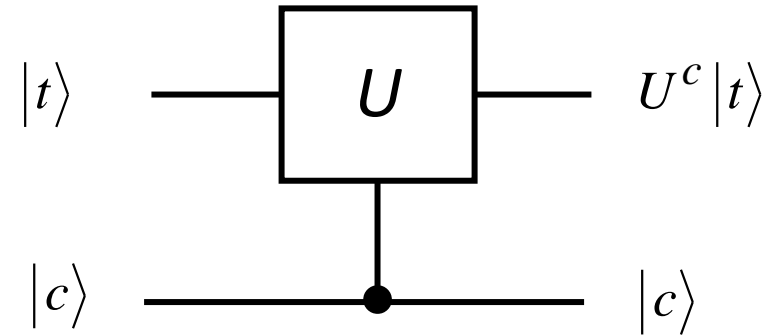
$$(c \uparrow)U|01\rangle = (U|0\rangle) \otimes |1\rangle = (U_{00}|0\rangle + U_{10}|1\rangle) \otimes |1\rangle = U_{00}|01\rangle + U_{10}|11\rangle$$

$$(c \uparrow)U|11\rangle = (U|1\rangle) \otimes |1\rangle = (U_{01}|0\rangle + U_{11}|1\rangle) \otimes |1\rangle = U_{01}|01\rangle + U_{11}|11\rangle$$

$$\begin{aligned} U|0\rangle &= U_{00}|0\rangle + U_{10}|1\rangle \\ U|1\rangle &= U_{01}|0\rangle + U_{11}|1\rangle \end{aligned}$$

and the matrix we obtain is

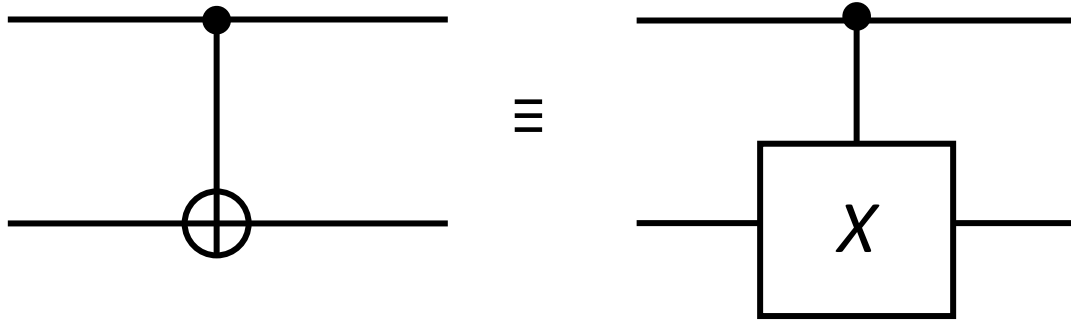
$$(c \uparrow)U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & U_{10} \\ 0 & 0 & 1 & 0 \\ 0 & U_{01} & 0 & U_{11} \end{bmatrix}$$



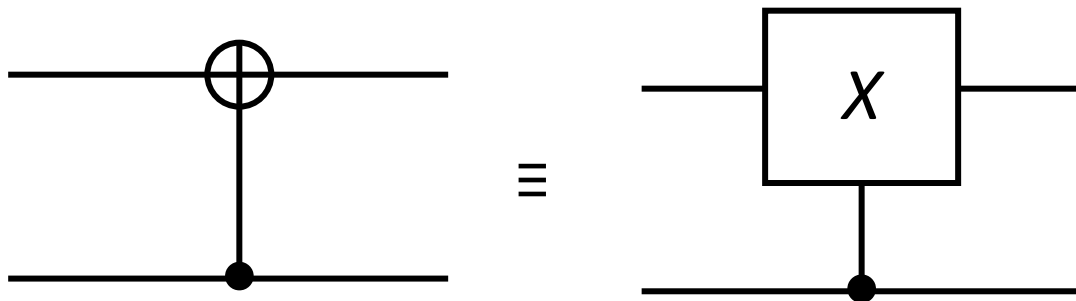
$$|t\rangle \rightarrow \begin{cases} |t\rangle & \text{If } c=0 \\ U|t\rangle & \text{If } c=1 \end{cases}$$

Swapping Roles in *controlled-U* Gate

- We have already proved that $CNOT = CX$



- Now, we want to calculate the matrix associated to $(C \uparrow)CNOT$



Swapping Roles in *controlled-U* Gate

$$(C \uparrow)U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & U_{10} \\ 0 & 0 & 1 & 0 \\ 0 & U_{01} & 0 & U_{11} \end{bmatrix}$$

- Since

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{matrix} U_{00} = U_{11} = 0 \\ U_{01} = U_{10} = 1 \end{matrix} \quad \longrightarrow \quad (C \uparrow)CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

- $(C \uparrow)CNOT$ is Hermitian, i.e. $(C \uparrow)CNOT = (C \uparrow)CNOT^\dagger$
- Furthermore, $(C \uparrow)CNOT$ is unitary, i.e.

$$[(C \uparrow)CNOT][(C \uparrow)CNOT]^\dagger = [(C \uparrow)CNOT]^\dagger[(C \uparrow)CNOT] = I$$

Swapping Roles in *controlled-U* Gate

Proof

$$[(c \uparrow)CNOT][(c \uparrow)CNOT]^\dagger = [(c \uparrow)CNOT]^\dagger [(c \uparrow)CNOT]$$

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

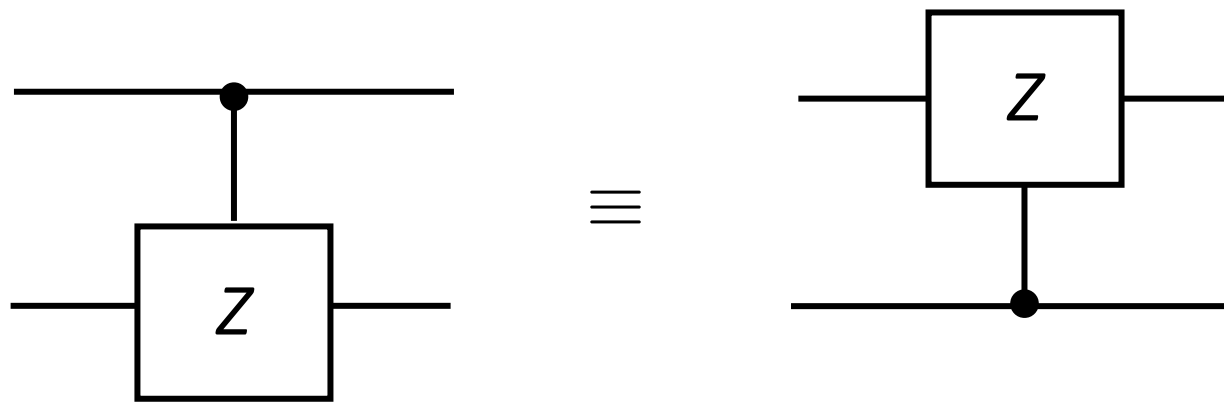
Swapping Roles in *controlled-U* Gate

- It is easy to show that

$$CNOT \cdot (C \uparrow) CNOT \cdot CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = SWAP$$

Swapping Roles in *controlled-U* Gate

- Furthermore



$$(C \uparrow)U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & U_{10} \\ 0 & 0 & 1 & 0 \\ 0 & U_{01} & 0 & U_{11} \end{bmatrix}$$

- In fact, from

$$U = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{matrix} U_{00} = 1 \\ U_{11} = -1 \\ U_{01} = U_{10} = 0 \end{matrix} \quad \longrightarrow \quad (C \uparrow)Z = CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Multi-Gate Circuits

- We have all the ingredients to make countless quantum circuits from the basic binary gates introduced above
- We'll start with the famous Bell states
- These are the only four **maximally** entangled pairs, and they are known as the *Bell states* or *EPR states* or *EPR pairs* (for the physicists Einstein, Podolsky, and Rosen)

A Circuit that Produces Bell States

- We've already met them

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

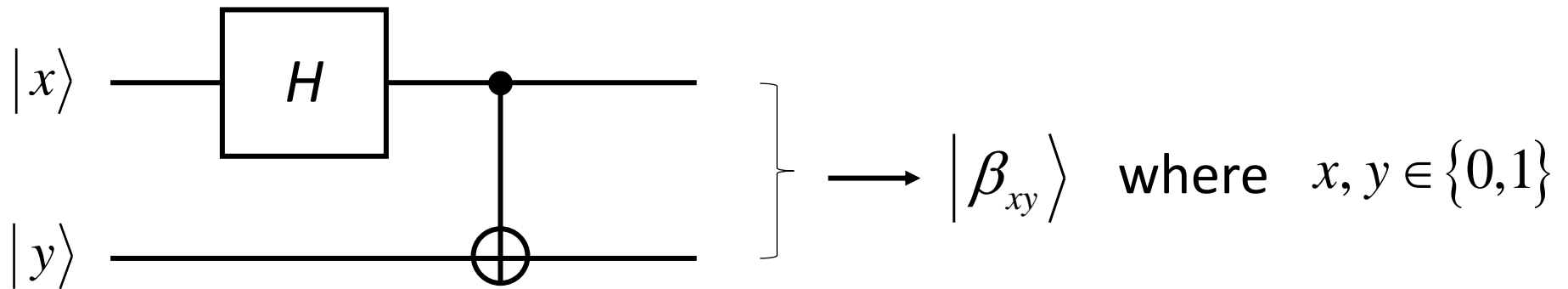
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \rightarrow |\Psi^+\rangle$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \rightarrow |\Phi^-\rangle$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \rightarrow |\Psi^-\rangle$$

A Circuit that Produces Bell States

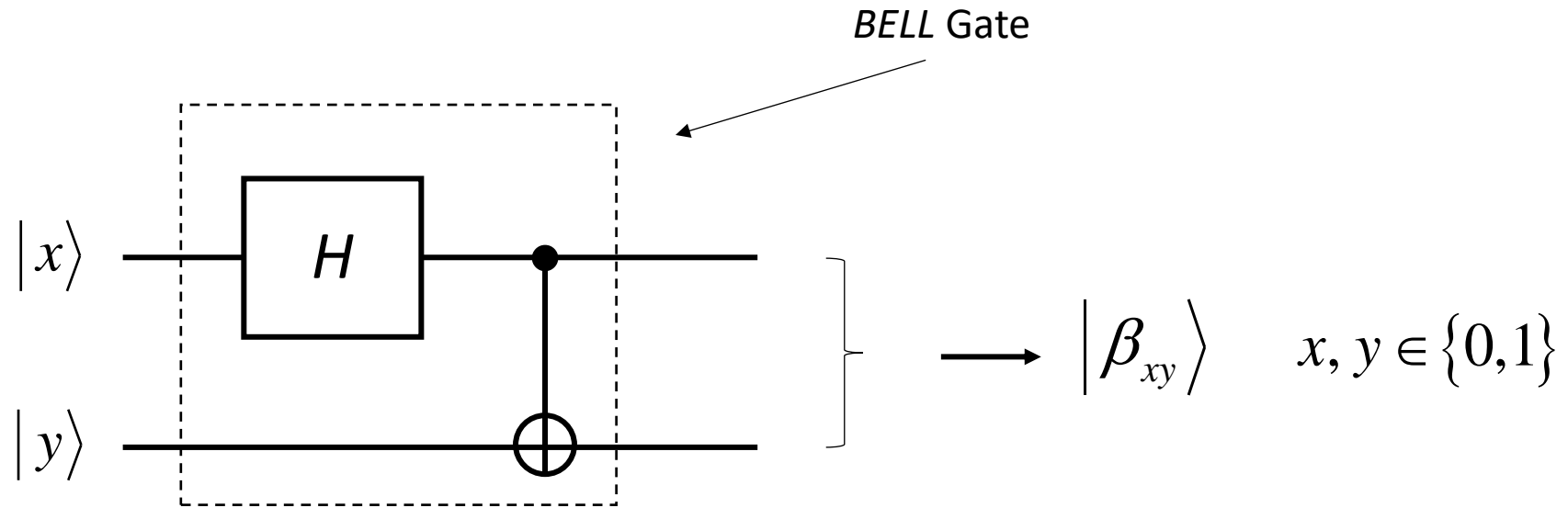
- The circuit that produces these four states, using the standard CBS basis as inputs $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$ is



which can be seen as a combination of a unary Hadamard gate with a CNOT gate

A Circuit that Produces Bell States

- We could emphasize that this is a binary gate in its own right by calling it BELL and boxing it



A Circuit that Produces Bell States

- In concrete terms, the algebraic expression,

$$BELL(|x\rangle|y\rangle) = |\beta_{xy}\rangle$$

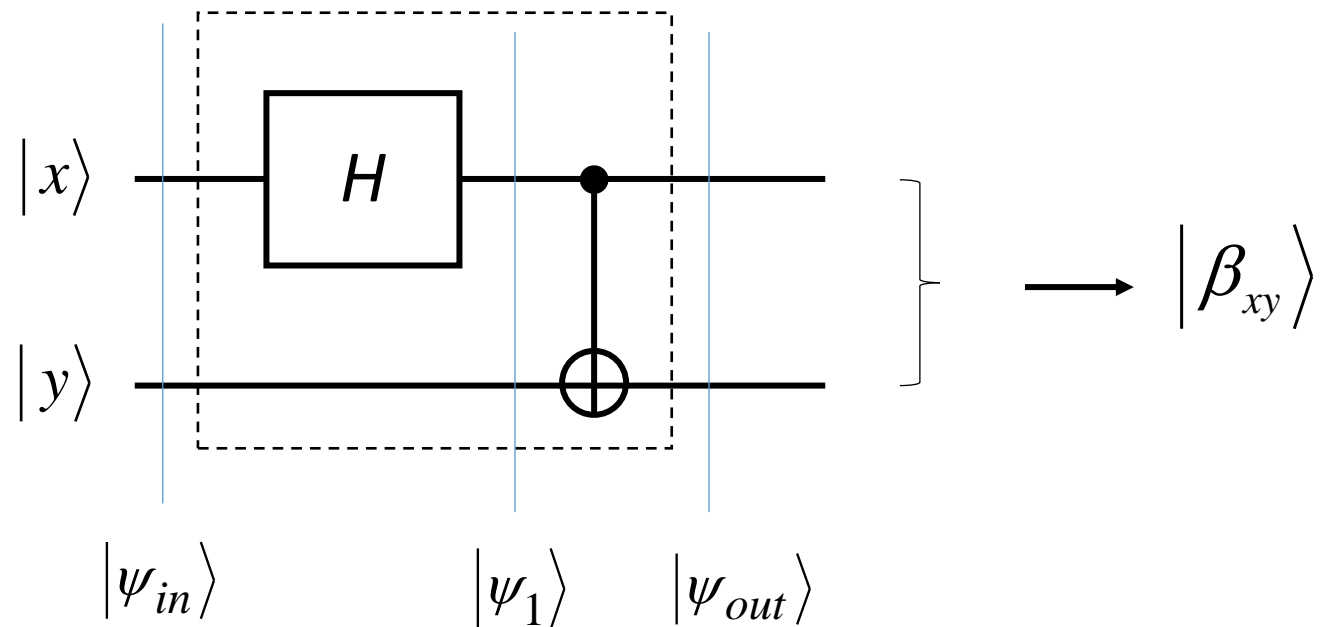
is telling us that

$$BELL(|0\rangle|0\rangle) = |\beta_{00}\rangle$$

$$BELL(|0\rangle|1\rangle) = |\beta_{01}\rangle$$

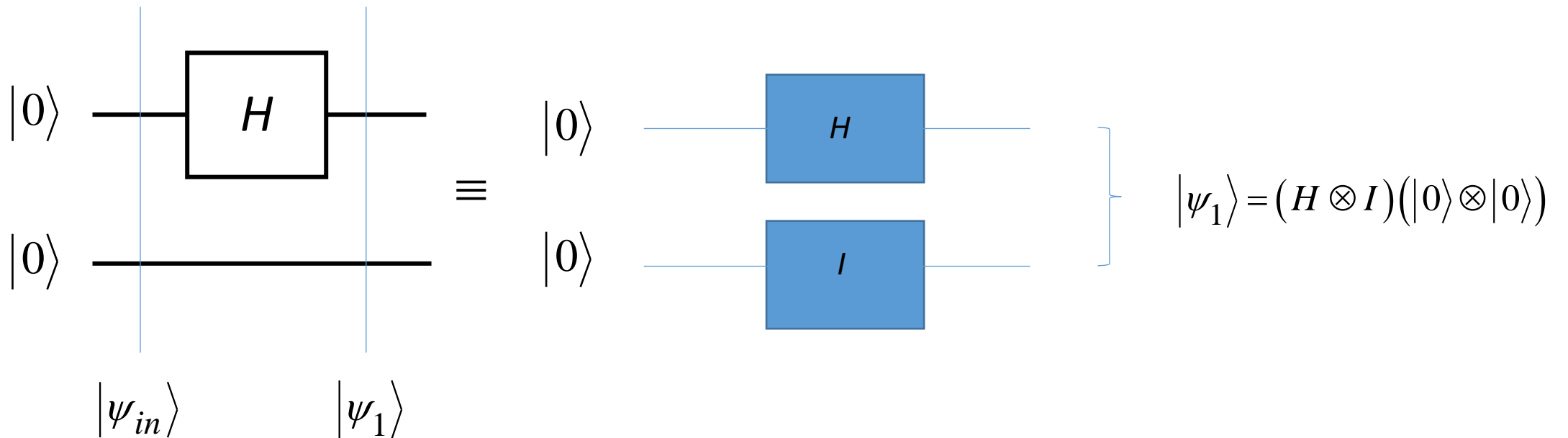
$$BELL(|1\rangle|0\rangle) = |\beta_{10}\rangle$$

$$BELL(|1\rangle|1\rangle) = |\beta_{11}\rangle$$



A Circuit that Produces Bell States

- Let's prove that

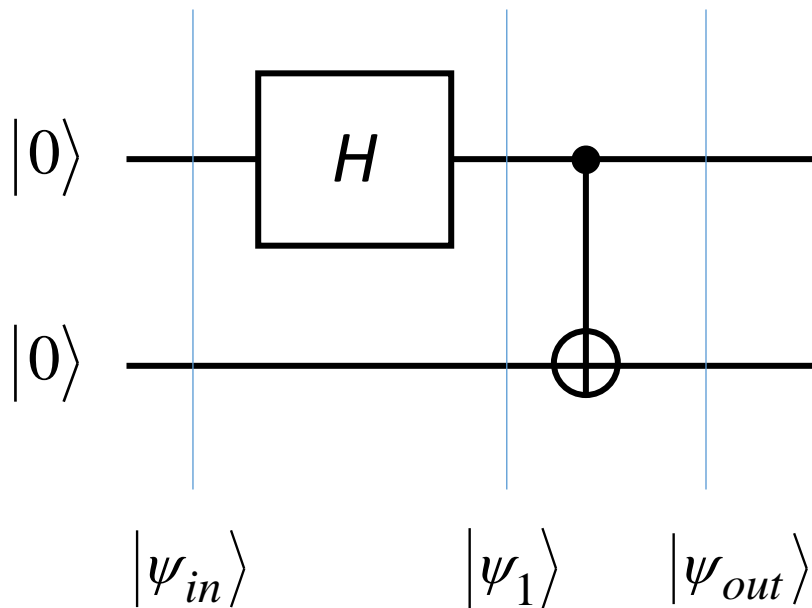


A Circuit that Produces Bell States

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

$\forall x \in \{0,1\}$

- Let's prove that $BELL(|0\rangle|0\rangle) = |\beta_{00}\rangle$



$$|\psi_{in}\rangle = |0\rangle|0\rangle$$

$$\begin{aligned} |\psi_1\rangle &= (H \otimes I)(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes I|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \end{aligned}$$

$$\begin{aligned} |\psi_{out}\rangle &= CNOT|\psi_1\rangle = \frac{1}{\sqrt{2}}(CNOT|00\rangle + CNOT|10\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\beta_{00}\rangle \end{aligned}$$

A Circuit that Produces Bell States

- We can easily prove that by following the same approach as before

$$BELL(|x\rangle|y\rangle) = |\beta_{xy}\rangle$$

for the others

$$x, y \in \{0,1\} \setminus \{0,0\}$$

- Thus

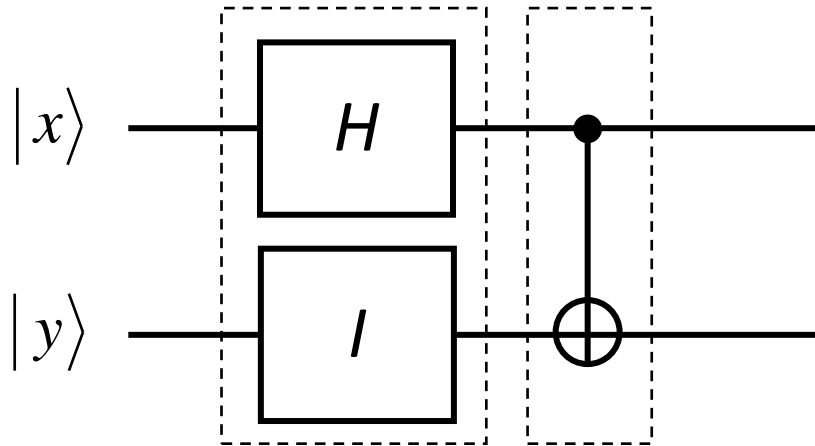
$$BELL = \begin{bmatrix} |\beta_{00}\rangle & |\beta_{01}\rangle & |\beta_{10}\rangle & |\beta_{11}\rangle \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

The Matrix for BELL

- The matrix for this gate can be constructed using the technique we have already illustrated in the previous slides
- For variety, let's now take a different path
- The Hadamard gate has a plain quantum wire below it, meaning that such a quantum wire is implicitly performing an identity operator at that point

The Matrix for BELL

- So we could write the gate using the equivalent symbolism



Explain why the order of the matrices is opposite the order of the gates in the diagram

$$BELL = (CNOT)(H \otimes I) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

The Matrix for BELL

- Let's apply the BELL matrix to the input state $|10\rangle$

$$BELL|10\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = \beta_{10}$$

- In general, it can be shown that the *BELL* matrix gives the four Bell states when one presents the four standard states as inputs

The Matrix for BELL Dagger

- It can also be proved easily that the *BELL* matrix is unitary
- Using the adjoint conversion rules, and remembering that the order of operators in the circuit is opposite of that in the algebra, we find

$$BELL^\dagger = [(CNOT)(H \otimes I)]^\dagger = (H \otimes I)^\dagger (CNOT)^\dagger = (H \otimes I)(CNOT)$$

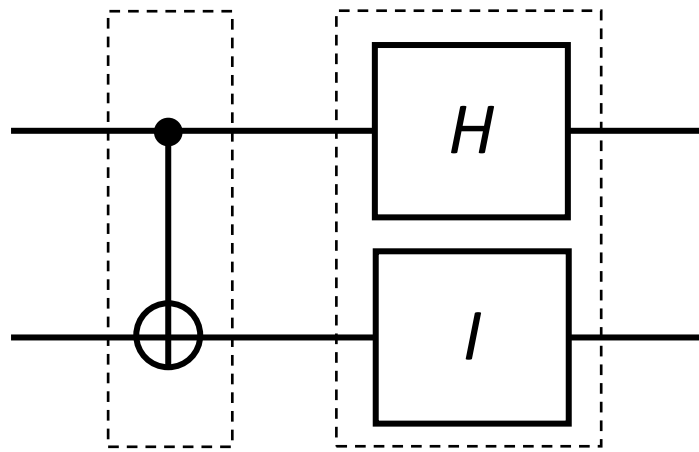
- The final equality is a consequence of the fact that CNOT and $H \otimes I$ are both self-adjoint and that

$$(H \otimes I)^\dagger = H^\dagger \otimes I^\dagger = H \otimes I$$

$$(CNOT)^\dagger = CNOT$$

The Matrix for BELL Dagger

- In other words, we just reverse the order of the two sub-operators that comprise BELL
- This makes the circuit diagram for $BELL^\dagger$ come out to be



$$BELL^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

The Matrix for BELL Dagger

- Now, by using $BELL$ and $BELL^\dagger$ matrices it is a matter of manipulating the matrices to prove that *the* $BELL$ matrix is unitary

$$BELL \times BELL^\dagger = \frac{1}{2} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

$$BELL^\dagger \times BELL = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

Four Bell States from One

- We can now list the following results

$$(I \otimes I)|\beta_{00}\rangle = |\beta_{00}\rangle$$

$$(X \otimes I)|\beta_{00}\rangle = |\beta_{01}\rangle$$

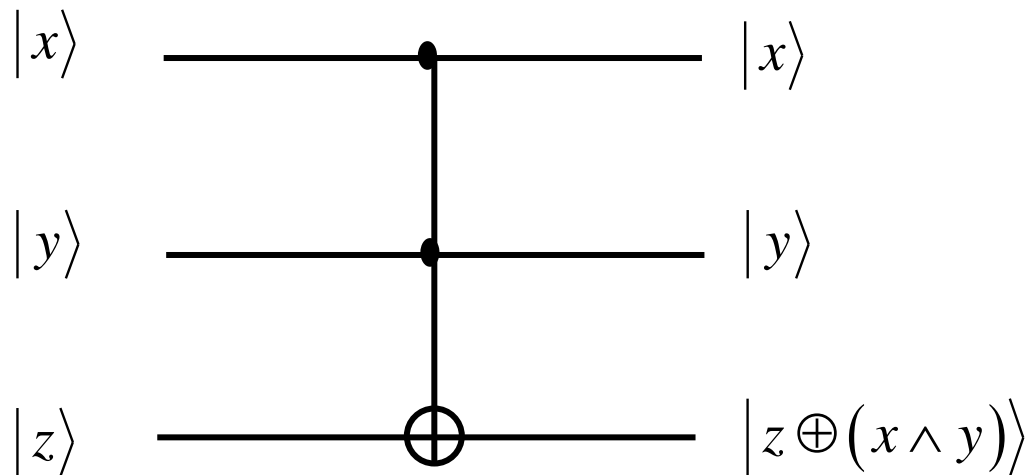
$$(Z \otimes I)|\beta_{00}\rangle = |\beta_{10}\rangle$$

$$(iY \otimes I)|\beta_{00}\rangle = |\beta_{11}\rangle$$

- Thus, a local operation on an entangled state changes the entire state, affecting both qubits of the entangled pair

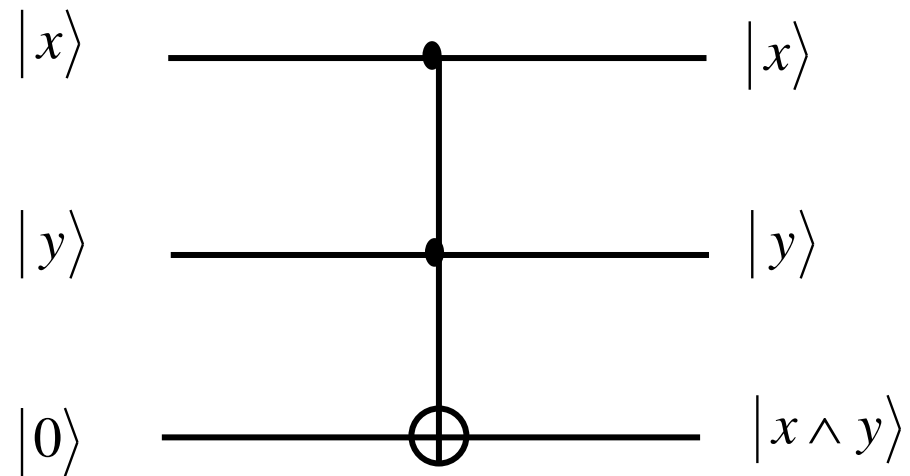
Toffoli Gate

- This is similar to the CNOT gate, but with two controlling bits
- The bottom bit flips only when *both* of the top two bits are in state $|1\rangle$
- We can write this operation as taking state $|x\rangle|y\rangle|z\rangle$ to $|x\rangle|y\rangle|z \oplus (x \wedge y)\rangle$



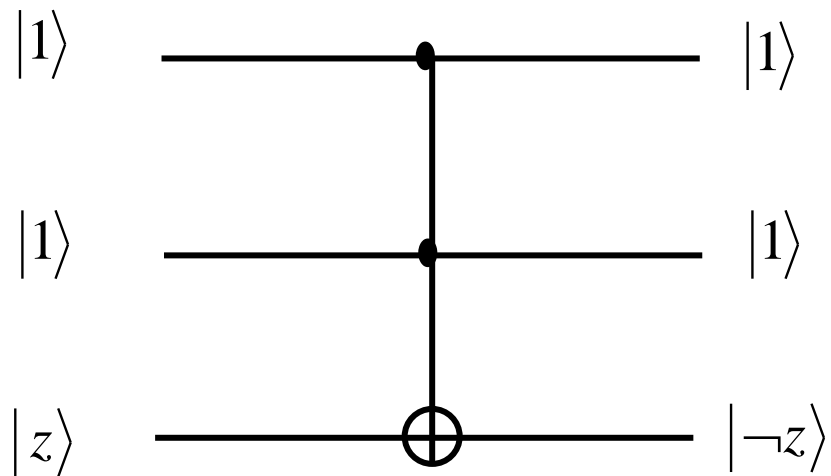
Toffoli Gate

- The *AND* gate is obtained by setting the bottom $|z\rangle$ input to $|0\rangle$

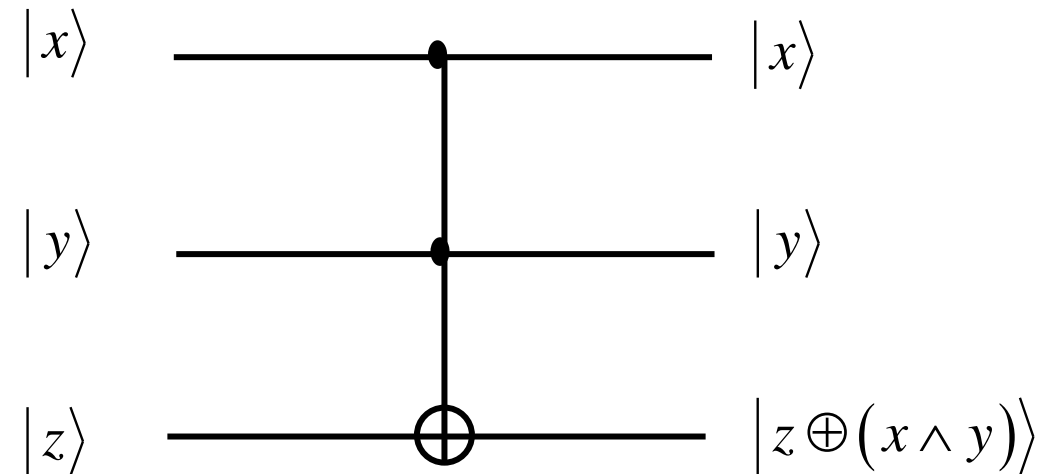


Toffoli Gate

- The *NOT* gate is obtained by setting the top two inputs to $|1\rangle$
- The bottom output will be $|(1 \wedge 1) \oplus z\rangle = |1 \oplus z\rangle = |\neg z\rangle$

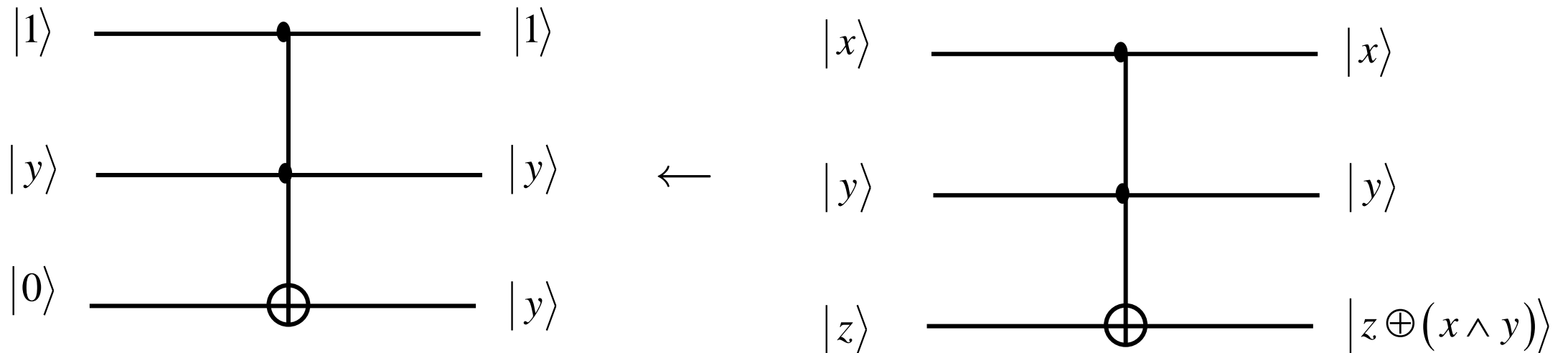


←



Toffoli Gate

- In order to construct all gates, we must also have a way of producing a fanout of values.
- In other words, a gate is needed that inputs a value and outputs two of the same values.
- This can be obtained by the following Toffoli setting



Toffoli Gate

- The Toffoli gate flips the right qubit if the left and middle qubits are 1

$$\text{Toffoli}|000\rangle = |000\rangle$$

$$\text{Toffoli}|001\rangle = |001\rangle$$

$$\text{Toffoli}|010\rangle = |010\rangle$$

$$\text{Toffoli}|011\rangle = |011\rangle$$

$$\text{Toffoli}|100\rangle = |100\rangle$$

$$\text{Toffoli}|101\rangle = |101\rangle$$

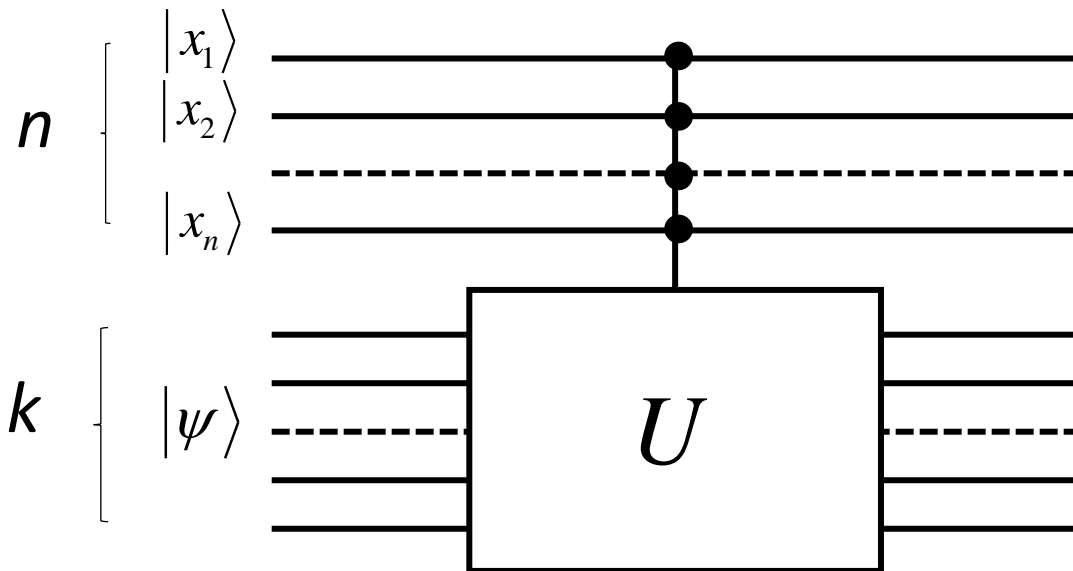
$$\text{Toffoli}|110\rangle = |111\rangle$$

$$\text{Toffoli}|111\rangle = |110\rangle$$

	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

Conditioning On Multiple Qubits

- Now that we know how to condition on a single qubit being set, what about conditioning on multiple qubits?
- More generally, suppose we have $n + k$ qubits, and U is a k qubit unitary operator



Then we define the controlled operation $C^n(U)$ by the equation

$$C^n(U) |x_1 x_2 x_3 \cdots x_n\rangle |\psi\rangle = |x_1 x_2 x_3 \cdots x_n\rangle U^{x_1 x_2 x_3 \cdots x_n} |\psi\rangle$$

Universal Set of Quantum Gates

- The gates we have seen so far have acted on either a single qubit, or on two qubits
- An interesting quantum algorithm would, in general, be some complicated unitary operator acting non-trivially on n -qubits
- In classical computing, we implement complicated operations as a sequence of much simpler operations
- In practice, we want to be able to select these simple operations from some set of elementary gates

Universal Set of Quantum Gates

- In quantum computing, we do the same thing
- The goal is to choose some **finite set of gates** so that, by constructing a circuit using only gates from that set, we can implement non-trivial and interesting quantum computations
- When we use a circuit of quantum gates to implement some desired unitary operation, in practice, it suffices to have an implementation that approximates the desired unitary to some specified level of accuracy
- We need to make precise the notion of the quality of an approximation of a unitary transformation

Universal Set of Quantum Gates

- Suppose we approximate a desired unitary transformation U by some other unitary transformation V
- The error in the approximation is defined to be

$$E(U, V) \equiv \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$$

- When we say that an operator U can be **'approximated to arbitrary accuracy'**, we mean that if we are given any *error tolerance* $\epsilon > 0$, we can implement some unitary V such that $E(U, V) < \epsilon$

Universal Set of Quantum Gates

- Also, we can show that if we perform a sequence of gates V_1, V_2, \dots, V_m intended to approximate some other sequence of gates U_1, U_2, \dots, U_m , then the errors add **at most linearly**,

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \leq \sum_{j=1}^m E(U_j, V_j)$$

Universal Set of Quantum Gates

- **Definition:** *A set of gates is said to be **universal** if for any integer $n \geq 1$, any n -qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set*
- Finding convenient universal sets of gates is of great practical importance as well as of theoretical interest
- *It is not within the scope of this course to discuss the topic of proving that a set of gates is universal*
- To be universal, a set of quantum gates must meet certain requirements, which we will elaborate on in the next slides

Universal Set of Quantum Gates

Interference/superposition

- We must be able to produce superpositions
- For example, the Hadamard gate can create superpositions, such as $H|0\rangle = |+\rangle$
- Other gates are not
 - > Z , S , and T only apply phases; they do not create superpositions of 0 and 1
 - > Similarly, the X and $CNOT$ gates only flip 0 and 1, so they cannot create superpositions
 - > Y only applies phases and flips, so again superpositions cannot be created by it

Universal Set of Quantum Gates

Entanglement

- We must be able to entangle qubits
- One-qubit gates, such as H , cannot do this since it only acts on a single qubit
- It must act on at least two qubits to produce entanglement
- $CNOT$ can produce entanglement since $CNOT|+\rangle|0\rangle = |\Phi^+\rangle$
- Not all two qubit gates produce entanglement, however
- The SWAP gate cannot generate entanglement since it only swaps two qubits

Universal Set of Quantum Gates

Complex Amplitudes

- *CNOT* and *H* only contain real numbers, so they do not produce states with complex amplitudes

Universal Set of Quantum Gates

Contain More than the Clifford Group

- The *Clifford group* is the set of gates $\{CNOT, H, S\}$ and although this set satisfies all of the previous requirements (entanglement, interference, and complex amplitudes), the *Gottesman-Knill theorem* says that a quantum circuit containing only these gates is efficiently simulated by a classical computer
- That is, the Clifford group is only as powerful as a classical computer, so a universal quantum gate set should contain more than this

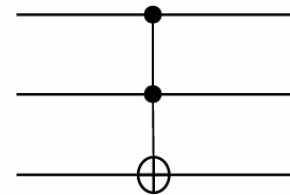
Universal Set of Quantum Gates

- It is unknown if these are sufficient requirements for a set of quantum gates to be universal
- It may be that a set satisfies all of these properties, but is still not universal

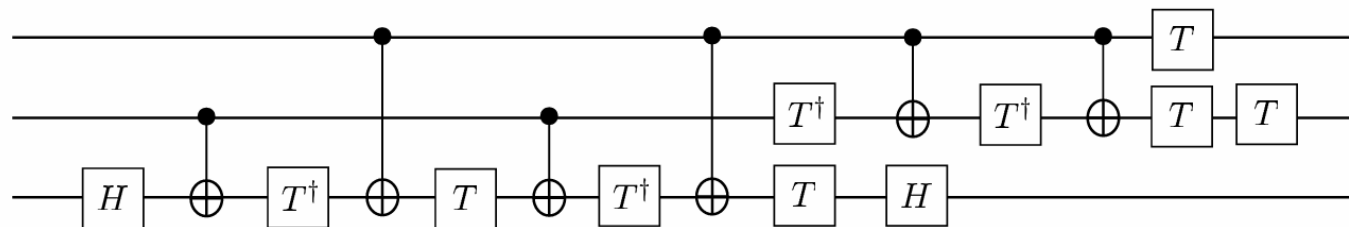
Examples of Universal Gate Sets

Some examples of universal gate sets are:

- $\{\text{CNOT}, \text{all single-qubit gates}\}$ is universal for quantum computing
- $\{\text{CNOT}, H, T\}$ is universal for quantum computing. That is, although the Clifford group $\{\text{CNOT}, H, S\}$ is *not* universal for quantum computing, replacing S with T is universal for quantum computing. H and T are sufficient to approximate all one-qubit gates.



||



Examples of Universal Gate Sets

- $CNOT, R_{\pi/8}, S$ is universal for quantum computing, where

$$R_{\pi/8} = \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & -\sin\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix}$$

- Although the Clifford group $\{CNOT, H, S\}$ is not universal for quantum computing, replacing H with $R_{\pi/8}$ is universal for quantum computing

Examples of Universal Gate Sets

- $CNOT, R_{\pi/8}, S$ is universal for quantum computing, where

$$R_{\pi/8} = \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & -\sin\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix}$$

- Although the Clifford group $\{CNOT, H, S\}$ is not universal for quantum computing, replacing H with $R_{\pi/8}$ is universal for quantum computing

Examples of Universal Gate Sets

- $\{\text{Toffoli}, H, S\}$ is universal for quantum computing. Although $\{\text{CNOT}, H, S\}$ is not universal for quantum computing, replacing CNOT with Toffoli is universal for quantum computing.
- H plus almost any two-qubit unitary

Solovay-Kitaev Theorem

- The Solovay-Kitaev theorem says that with **any universal gate set**, we can approximate a quantum gate on **n** qubits to precision ε using $\Theta(2^n \log^c 1/\varepsilon)$ gates for some constant **c**
- The dependence on the number of qubits 2^n is what we might expect since an operator on **n** qubits is a matrix of $2^n \times 2^n$ entries.
- The dependence on the precision $\log^c 1/\varepsilon$ is great!
- The precision is the “distance” (in some measurement or metric) that the approximate quantum gate is to the actual quantum gate, and we want it to be small

Solovay-Kitaev Theorem

- So $1/\varepsilon$ is big, but taking the logarithm of it makes it small.
- A logarithm to a constant power is a polynomial of a logarithm, so \log^c is also called polylog. This is also considered small
- Thus, this dependence means our approximation quickly converges on the actual quantum gate

NOTE

- $f(n) = \Theta(g(n))$, means there exists constants c_1 , c_2 , and n_0 such that

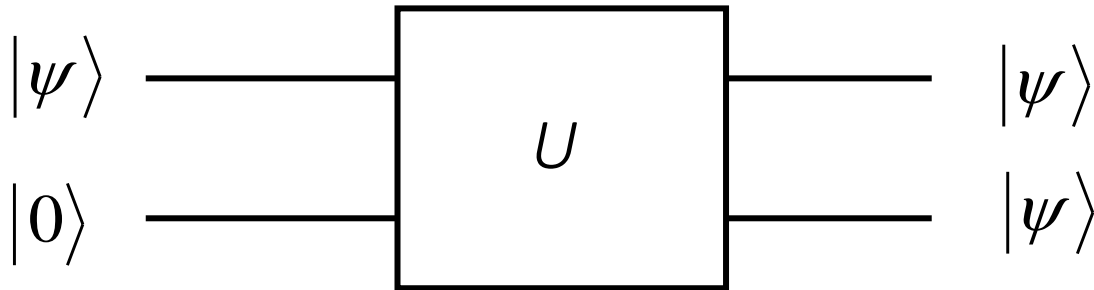
$$c_1 g(n) \leq f(n) \leq c_2 g(n)$$

for all values of n greater than n_0

No-Cloning Theorem

No-Cloning Theorem

- Is it possible to make a copy of an *unknown* quantum state?
- Surprisingly, it turns out that the answer to this question is *NO*
- Suppose we try to copy a qubit in the *unknown* state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$



or

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

No-Cloning Theorem

- By using linear algebra

$$\begin{bmatrix} U_{00} & U_{01} & U_{02} & U_{03} \\ U_{10} & U_{11} & U_{12} & U_{13} \\ U_{20} & U_{21} & U_{22} & U_{23} \\ U_{30} & U_{31} & U_{32} & U_{33} \end{bmatrix} \left(\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

- Since

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \beta\alpha \\ \beta^2 \end{bmatrix} \quad \longrightarrow$$

No-Cloning Theorem

$$\begin{bmatrix} U_{00} & U_{01} & U_{02} & U_{03} \\ U_{10} & U_{11} & U_{12} & U_{13} \\ U_{20} & U_{21} & U_{22} & U_{23} \\ U_{30} & U_{31} & U_{32} & U_{33} \end{bmatrix} \begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{bmatrix} \longrightarrow \begin{bmatrix} U_{00}\alpha + U_{02}\beta \\ U_{10}\alpha + U_{12}\beta \\ U_{20}\alpha + U_{22}\beta \\ U_{30}\alpha + U_{32}\beta \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{bmatrix}$$

There are many possible solutions, such as

$$\begin{array}{c|c} U_{00} = \alpha, & U_{02} = 0, \\ \hline U_{20} = 0, & U_{22} = \alpha, \end{array} \begin{array}{c|c} U_{10} = 0, & U_{12} = \alpha \\ \hline U_{30} = 0, & U_{32} = \beta \end{array} \longrightarrow$$

but this requires knowing α and β ,
which we do not know

Any general solution requires α and β , so there is no operator U that allows us to copy a general, *unknown* quantum state

No-Cloning Theorem

$$\begin{aligned} U_{00} &= \alpha, & U_{02} &= 0, & U_{10} &= 0, & U_{12} &= \alpha \\ U_{20} &= 0, & U_{22} &= \alpha, & U_{30} &= 0, & U_{32} &= \beta \end{aligned}$$

- Based on the results obtained previously the U matrix is

$$U = \begin{bmatrix} \alpha & U_{01} & 0 & U_{03} \\ 0 & U_{11} & \alpha & U_{13} \\ 0 & U_{21} & \alpha & U_{23} \\ 0 & U_{31} & \beta & U_{33} \end{bmatrix}$$

- Now assume that *we know* the state that we want to clone, e.g.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \longrightarrow \quad \alpha = \beta = \frac{1}{\sqrt{2}}$$

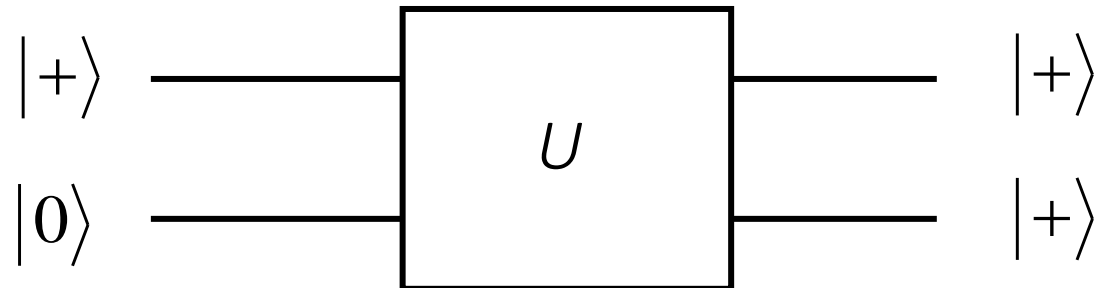
No-Cloning Theorem

- Therefore

$$U = \begin{bmatrix} 1/\sqrt{2} & U_{01} & 0 & U_{03} \\ 0 & U_{11} & 1/\sqrt{2} & U_{13} \\ 0 & U_{21} & 1/\sqrt{2} & U_{23} \\ 0 & U_{31} & 1/\sqrt{2} & U_{33} \end{bmatrix}$$

- Let's verify that

$$U(|+\rangle|0\rangle) = |+\rangle|+\rangle \quad \longrightarrow$$



No-Cloning Theorem

Since

$$|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \longrightarrow$$

$$U(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1/\sqrt{2} & U_{01} & 0 & U_{03} \\ 0 & U_{11} & 1/\sqrt{2} & U_{13} \\ 0 & U_{21} & 1/\sqrt{2} & U_{23} \\ 0 & U_{31} & 1/\sqrt{2} & U_{33} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = |+\rangle|+\rangle$$

Thus, we can produce additional copies of $|+\rangle$

No-Cloning Theorem

- Assume there is a unitary U that is able to clone qubits in two **known** states $|\psi\rangle$ and $|\phi\rangle$, i.e.,

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

$$U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$$

- For example, an operator that can clone both $|0\rangle$ and $|1\rangle$ is CNOT, since

$$\text{CNOT}|00\rangle = |00\rangle$$

$$\text{CNOT}|10\rangle = |11\rangle$$

- Taking the inner product of the previous two equations

No-Cloning Theorem

$$\langle \psi | \langle 0 | U^\dagger U | \phi \rangle | 0 \rangle = (\langle \psi | \langle \psi |) (| \phi \rangle | \phi \rangle)$$

\downarrow

$$\langle \psi | \langle 0 | I | \phi \rangle | 0 \rangle = (\langle \psi | \langle \psi |) (| \phi \rangle | \phi \rangle)$$

$$\langle \psi | \phi \rangle \langle 0 | 0 \rangle = \langle \psi | \phi \rangle \langle \psi | \phi \rangle$$

$$\langle \psi | \phi \rangle = (\langle \psi | \phi \rangle)^2$$

- For $\langle \psi | \phi \rangle$ to be equal to its square, it must be equal 0 or 1
- Thus $|\psi\rangle = |\phi\rangle$, or $|\psi\rangle$ and $|\phi\rangle$ are orthogonal
- Thus, an operator can only clone states that are orthogonal

Homework

- Does there exist a quantum operator U that can clone both
 1. $|+\rangle$ and $|-\rangle$?
 2. $|i\rangle$ and $|-i\rangle$?
 3. $|0\rangle$ and $|+\rangle$?