Quantum Information

Lecture #5

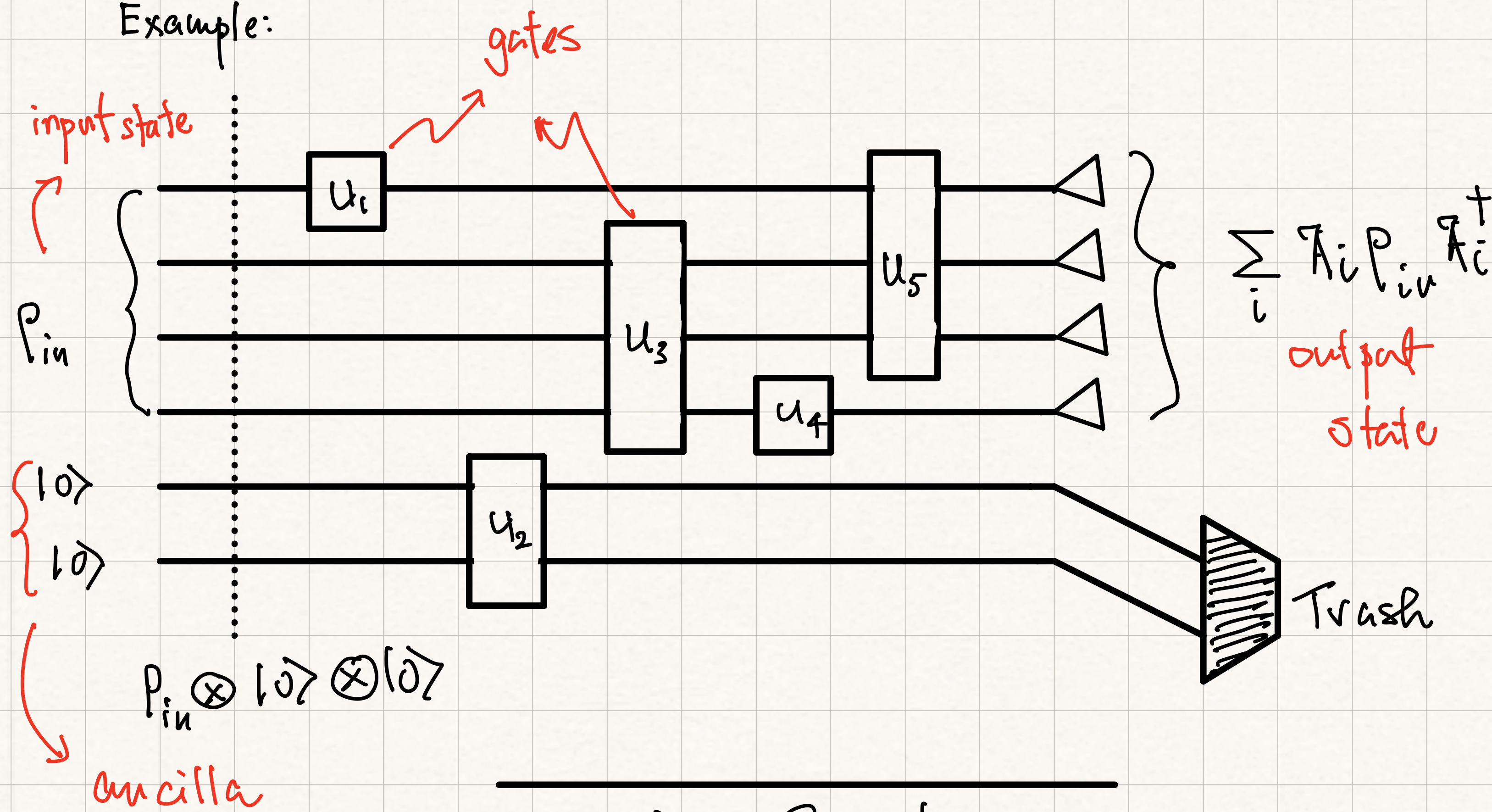
The Circuit Model of Quantum Computation

In the circuit model of quantum computation we have our logical qubits that are carried by wires. The physical realization of a qubit may involve many component systems (physical qubits).

As the qubits move from left to right with time unitary operators act on them. In quantum computation we call them gates. Unitary operations are reversible and so we use gates which are reversible. This is in contrast with classical gates which can be irresible.

Measurements on the qubits are usually done in the computational basis and they are denoted by $-\!\triangleleft$ symbol. Depending on the operation we are interested in we can have gates that act on one or more qubits.

Example:



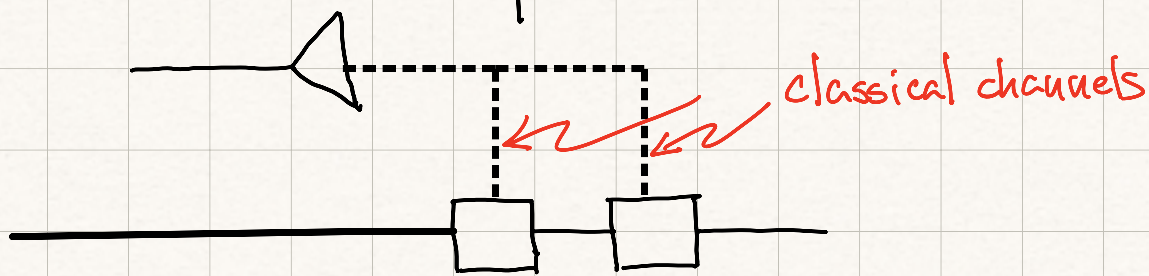
A Mockup of a Quantum Circuit

Ancilla qubits:

Often in quantum computation we require extra 'scratch' bits which help with the computation but which are discarded at the end of computation. Such bits are known as ancilla bits and they are usually initialized in the $|0\rangle$ state.

Classical channels:

In addition to wires through which quantum states propagate, sometimes we make a measurement and use the result of the measurement in a quantum computation down the line. We denote these classical channels by dashed lines:



Converting classical gates into quantum gates

Since quantum gates are reversible, when we are converting a classical circuit component to its quantum counterpart, we may have to carry extra information. E.g. the classical NOT gate is reversible:

NOT-gate

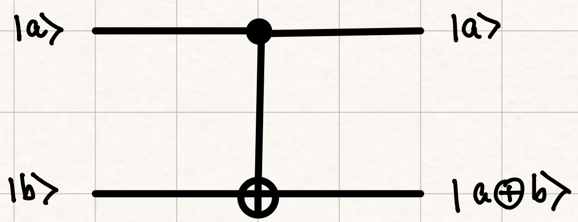
$$\text{NOT}: x \to x \oplus 1.$$

So it is easy to implement quantum mechanically:

since $X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

XOR (CNOT : Controlled NOT)



a	b	a	$a \oplus b$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Reversible.

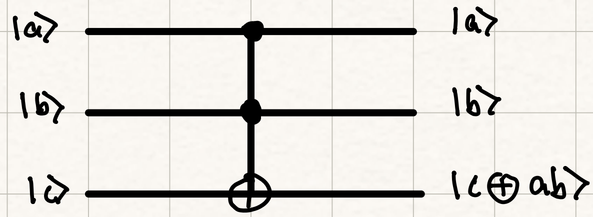
AND

a	b	$a \wedge b = ab \bmod 2$
0	0	0
0	1	0
1	0	0
1	1	1

Not Reversible!

We implement the AND gate as a Toffoli gate

Toffoli Gate



AND

a	b	c	a	b	$c \oplus ab$
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

We can represent quantum gates as matrices expressed in the computational basis:

CNOT : $|a, b\rangle \rightarrow |a, a \oplus b\rangle$ $\qquad$ $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Universal Gate Set:

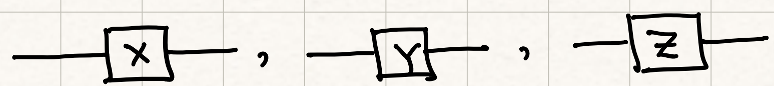
A gate set S is __universal__ if $\exists$ a product of gates from S which gives an arbitrary unitary $U \in SU(2^N)$.

\# For classical computation: Toffoli is universal

\# For quantum computation: $\{CNOT, \text{ all single-qubit rotations} \in SU(2)\}$

CNOT is a two qubit gate.

Examples of one-qubit gates: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$



Hadamard Gate:

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

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

$H^\dagger = H$ and $H^2 = 1$.

Phase rotation


$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$R_\theta|0\rangle = |0\rangle$$
$$R_\theta|1\rangle = e^{i\theta}|0\rangle$$

Comment:

1. We only need to define the action of a gate on the computational basis. The action of the gate on all other states follow by linearity. E.g.,

$$R_\theta : \alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + e^{i\theta}\beta|1\rangle$$

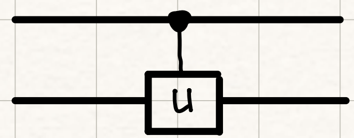
2. It may appear that a universal gate set must include an infinite variety of one qubit gates but that is not necessary. A set of 1-qubit gates is said to be universal for 1-qubit gates if any one qubit gate can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set.

3. The $\frac{\pi}{8}$-phase gate is given by $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ [which is equivalent to $\begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$]. Then the set $\{H, T\}$ is universal for 1-qubit gates.

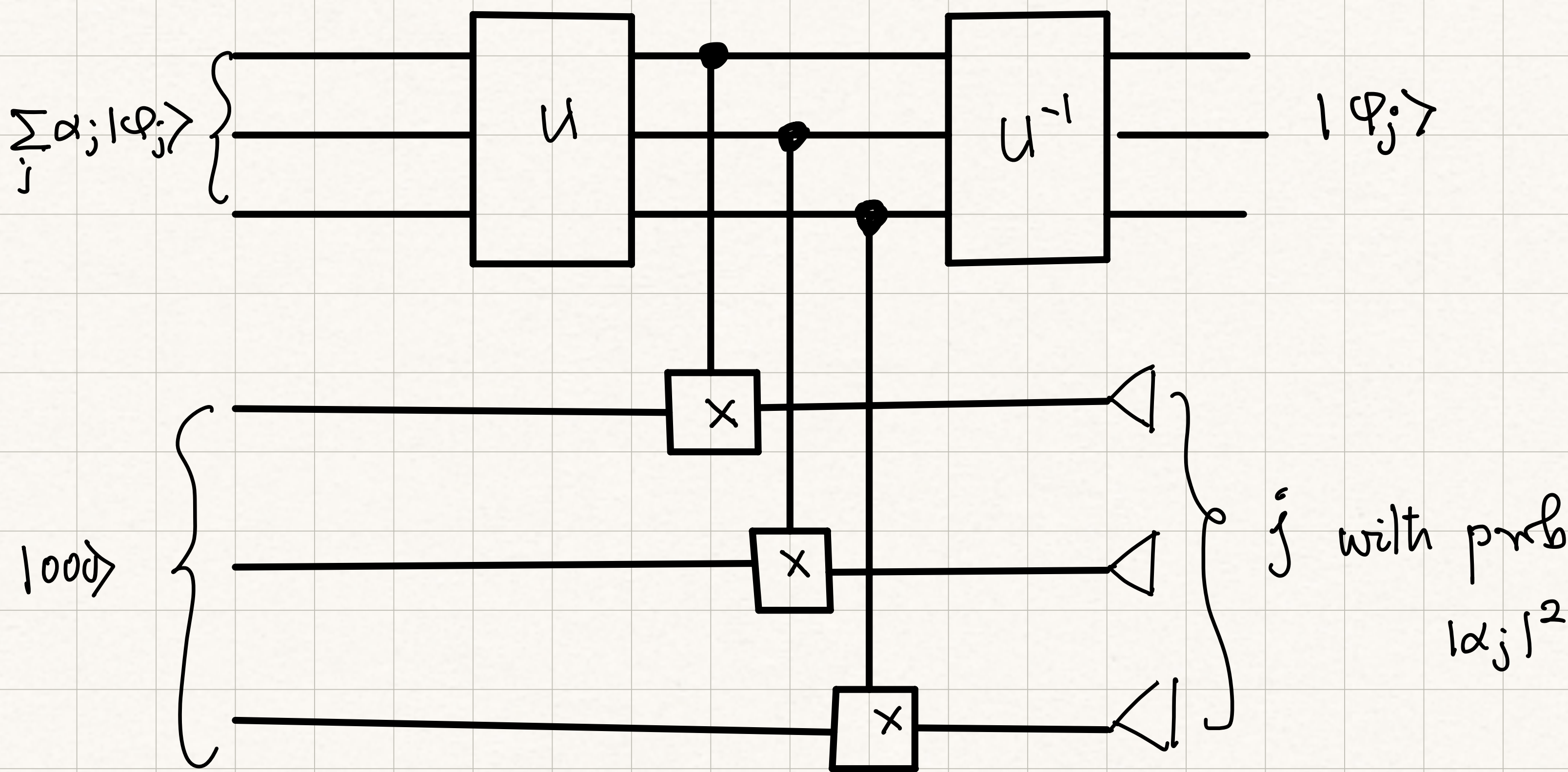
4. The set $\{CNOT, H, T\}$ is a universal set of gates.

Controlled-U gate:

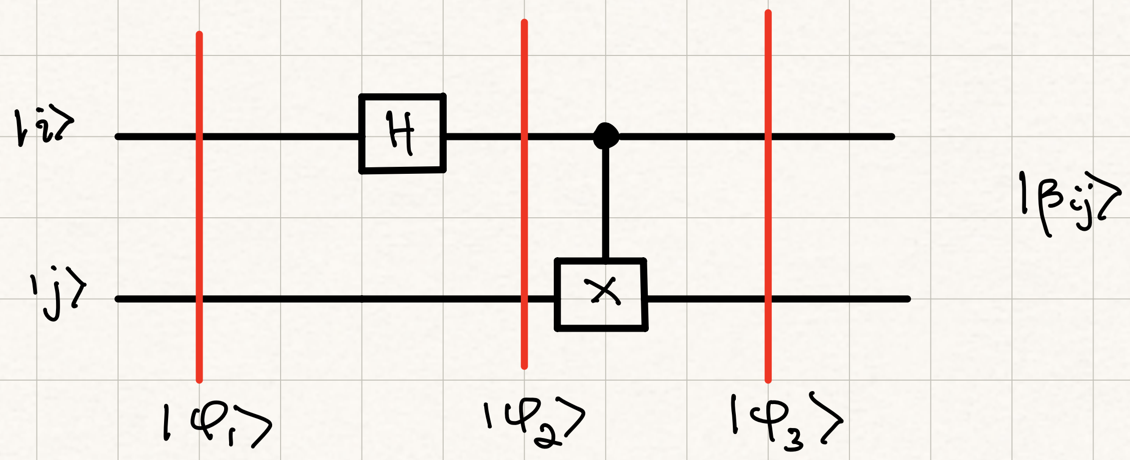
The CNOT gate can be generalized by replacing the NOT operation by any U



von-Neumann Measurement Circuit:



How to Make the Bell Basis?



$$|\varphi_1\rangle = |ij\rangle$$

$$|\varphi_2\rangle = (H \otimes \mathbb{1})\,|i,j\rangle = \frac{1}{\sqrt{2}}\left[(-1)^i|i\rangle + |\bar{i}\rangle\right] \otimes |j\rangle \qquad \{\text{ where } \bar{i} = i \oplus 1\}$$

$$= \frac{1}{\sqrt{2}}\left[(-)^i\,|ij\rangle + |\bar{i}\,j\rangle\right]$$

Next we apply CNOT on $|\varphi_2\rangle$ and get:

$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}\left[(-)^i\,|i, i\oplus j\rangle + |\bar{i}, \bar{i}\oplus j\rangle\right] = |\beta_{ij}\rangle$$

Thus we see $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}[-|11\rangle + |00\rangle] = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle]$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}[-|10\rangle + |01\rangle] = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]$$

Superdense Coding:

Suppose Alice wants to send Bob two classical bits. If Alice and Bob share an entangled state Alice can accomplish this task with sending just one qubit.

Suppose the entangled state is

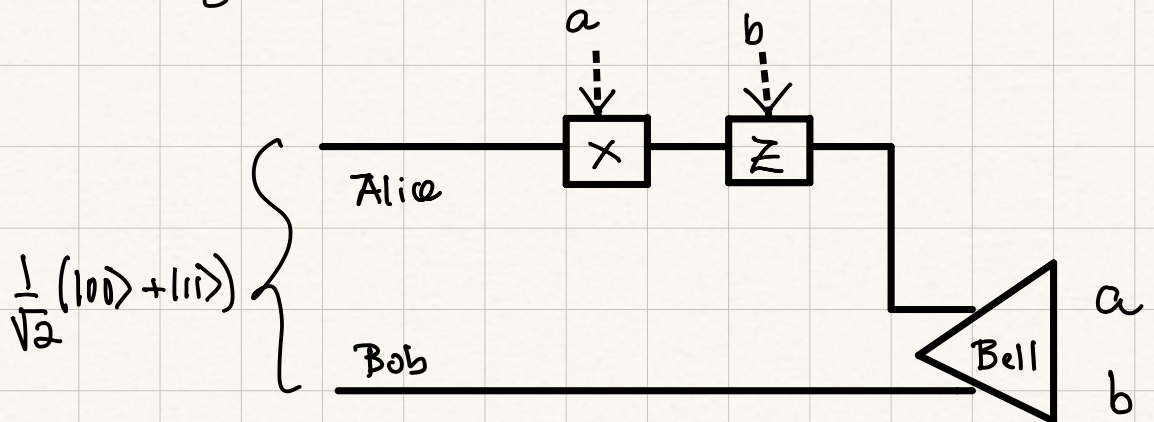
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Then to send the following classical bits Alice applies the following transformations

$$\begin{array}{c|l} 00 & I \otimes I\, |\beta_{00}\rangle = |\beta_{00}\rangle \\ 01 & X \otimes I\, |\beta_{00}\rangle = (X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\beta_{01}\rangle \end{array}$$

$$\begin{array}{c|l} 10 & Z\otimes I\,|\beta_{00}\rangle = (Z\otimes I)\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) = |\beta_{10}\rangle \\ 11 & (Z\cdot X\otimes I)|\beta_{00}\rangle = (Z\cdot X\otimes I)\,\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = \frac{1}{\sqrt{2}}\left(-|10\rangle+|01\rangle\right) = |\beta_{11}\rangle \end{array}$$

Then Bob just have to do a measurement in the Bell basis.



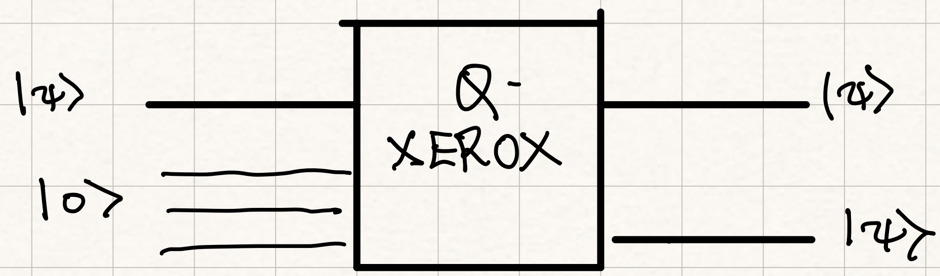
Quantum Teleportation

An often used 'subroutine' in quantum algorithms is quantum teleportation which allows Alice to send a qubit to Bob by using an entangled pair. Suppose Alice has a qubit in some unknown state $|\psi\rangle$ that she wants to send to Bob who is far away from her.

If Alice could copy her qubit $|\psi\rangle$ then she could send a copy. But quantum mechanics does not allow for a cloning machine to exist. This is a simple consequence linearity.

Proof of No Cloning Theorem:

Suppose such a machine exists.

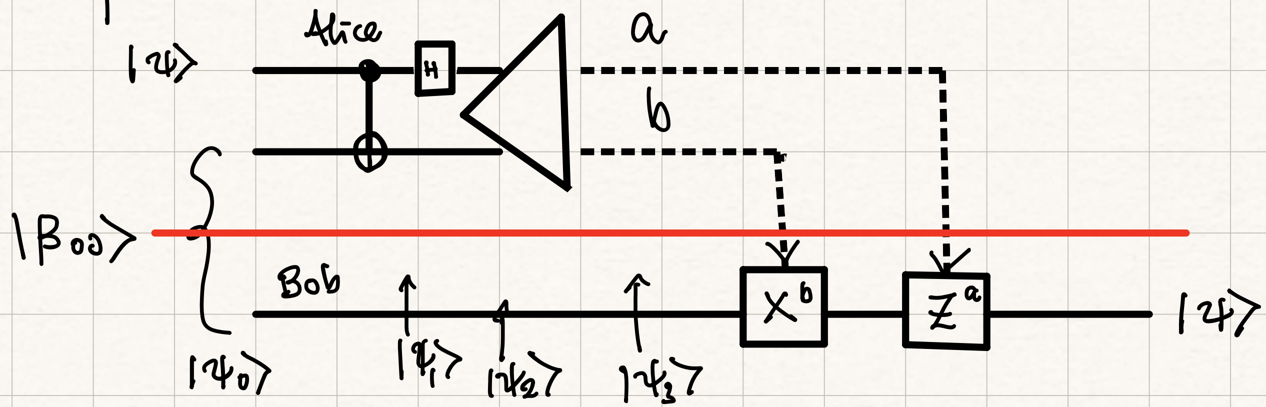


Then its action the computational basis would be
$$|0\rangle \to |0\rangle|0\rangle$$
$$|1\rangle \to |1\rangle|1\rangle$$

Now if we feed it an arb. qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then by linearity we get $\alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$.

Thus such a machine does not exist.

Teleportation:



Alice and Bob's initial state

$$|\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

After CNOT we get:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

Then we apply H on the first qubit

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

$$= \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle)\right.$$

$$+ |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

After measurement by Alice and BOB:

$$00 \longrightarrow |\psi_3\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$01 \longrightarrow |\psi_3\rangle = \alpha|1\rangle + \beta|0\rangle$$

$$10 \longrightarrow |\psi_3\rangle = \alpha|0\rangle - \beta|1\rangle$$

$$11 \longrightarrow |\psi_3\rangle = \alpha|1\rangle - \beta|0\rangle$$

Bob then applies the following operators conditional on the result of the joint measurement:

$$00: \quad I(\alpha|0\rangle + \beta|1\rangle) = |\psi\rangle$$

$$01: \quad X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$10: \quad Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$11: \quad ZX(\alpha|1\rangle - \beta|0\rangle) = Z(\alpha|0\rangle - \beta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle) = |\psi\rangle.$$

Phase Kick-Back

Consider the CNOT gate: $|a\rangle|b\rangle \rightarrow |a\rangle|a\oplus b\rangle$

Written in terms of the computational basis it appears that the first qubit is just a spectator qubit.

But if we feed it different states in the 'target' bit we get something very different:

$$\text{CNOT}: |0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \rightarrow |0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \rightarrow |1\rangle\left(\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right)$$

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

Which we can summarize as

$$\text{CNOT}: |a\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \rightarrow (-)^a|a\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).$$

Suppose we have a unitary operator U_f which implements the function:

$$f:\{0,1\} \rightarrow \{0,1\}$$

as a controlled-U_f gate:

$$C\text{-}U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$$

Then we can generalize phase kick-back by

$$U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \longrightarrow \frac{U_f|x\,0\rangle - U_f|x\,1\rangle}{\sqrt{2}}$$

$$= \frac{|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle}{\sqrt{2}}$$

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

If $f(x) = 0$ then it has no effect. But if $f(x) = 1$, then it leads to bit flip. Thus we get:

$$C\text{-}U_f : |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow (-)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

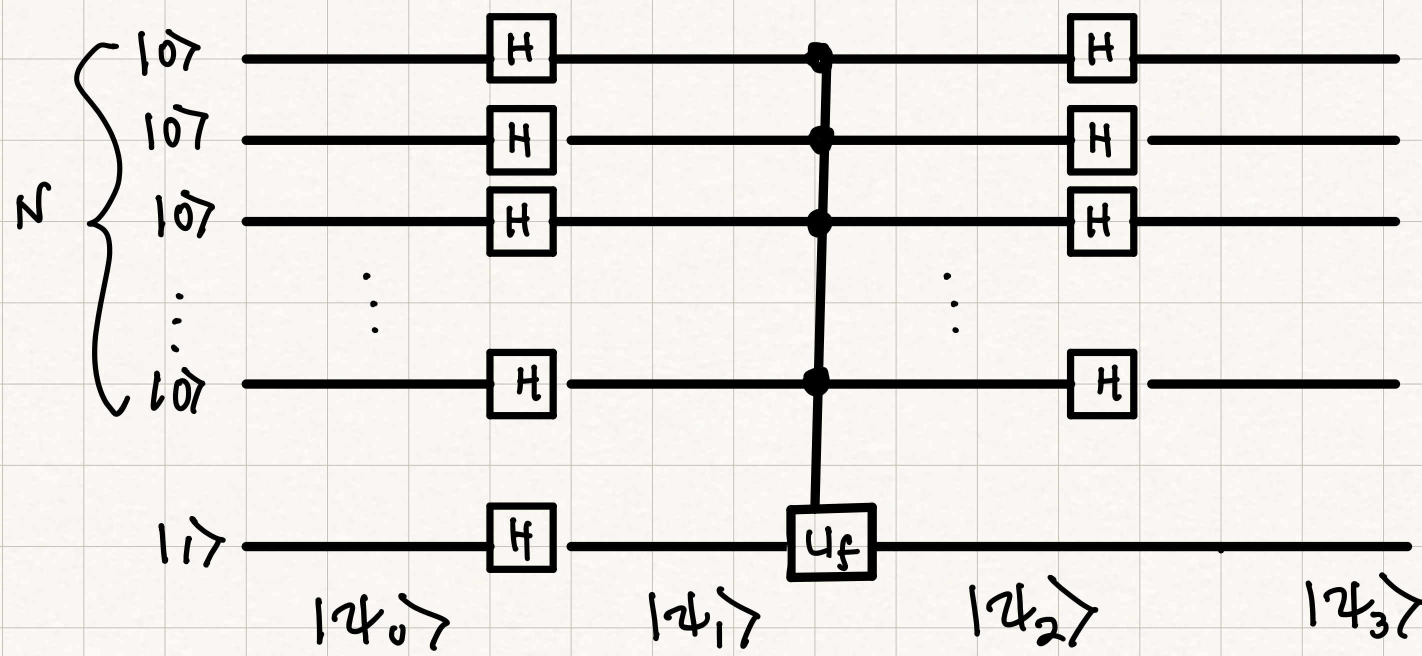
The Deutsch-Jozsa Algorithm:

The Deutsch problem is a toy problem that demonstrates the massive parallelism of quantum computing but also shows a limitation on the kind of measurements that is useful.

Suppose f is a function of $x \in \{0, 1, \ldots, 2^N - 1\}$ such that f is either a constant function or it is a balanced function, i.e. $f(x) = 0$ for half of the values of x, while it is $f(x) = 1$ for the other half of the values of x.

The problem is to find out whether it's a balanced function or not. The best classically deterministic algorithm has to invoke at most $2^{N-1}+1$ calls of $f(x)$ to determine whether $f(x)$ is balanced or not.

There exists a quantum algorithm that can solve this problem by one call of the function. The trick is to prepare a state that is the sum $\sum_x |x\rangle$, $\forall x \in \{0, 1, .., 2^N-1\}$. Then the function $f(x)$ can act on all values of its argument with just one call.



$$|\psi_0\rangle = |0 \ldots 0\rangle|1\rangle \longrightarrow |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)^{\otimes N} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Phase kickback

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^N}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$|\psi_3\rangle$ will depend on the nature of $f(x)$. If $f(x)$ is a constant function that all the phases $(-)^{f(x)}$ will be either $+1$ or -1. And the action on $H^{\otimes N}$ on $\sum_x |x\rangle$ will yield $|0\cdots 0\rangle$. In this case an observation of the first N qubits will all yield 0.

On the other hand if $f(x)$ is balanced then the positive and negative contributions to the $|0\ldots 0\rangle$ state will cancel and an observation of the first N qubits will yield some 1 values.