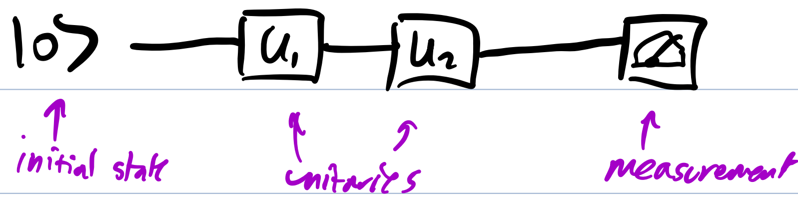
A 1-qubit quantum circuit looks like



This represents a sequence of operations on the quantum system $V = \mathbb{C}^2$ spanned by $|0\rangle, |1\rangle$

NOT gate $\oplus$ $\quad |0\rangle \mapsto |1\rangle$

or, X gate $\boxed{X}$ $\quad |1\rangle \mapsto |0\rangle$

Hadamard gate $\boxed{H}$ $\quad |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Want a circuit that transforms

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

Answer looks like this:

$$-\boxed{U_1}-\boxed{U_2}-\boxed{U_3}-$$

This is a composite gate

called the $\boxed{Z}$ gate.

We have shown that

$$-\boxed{Z}- \;=\; -\boxed{H}-\oplus-\boxed{H}-$$

$$Z = HXH$$

Key identity: $H^2 = 1$

If we apply X to

the vectors $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

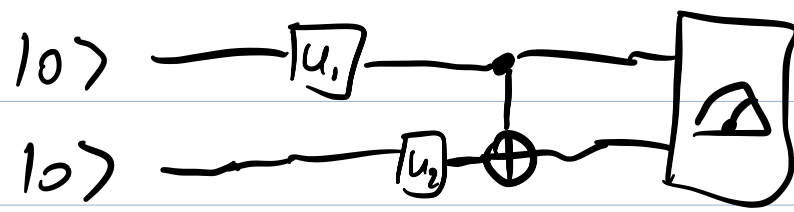
then X acts by multiplication, by 1 and -1

respectively.

We say that X is diagonal in the Hadamard basis.

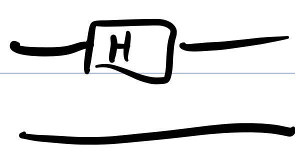
We say that H diagonalizes X

2-qubit quantum circuits



How do we interpret 1-qubit gates in a 2-qubit circuit?

e.g.



must represent an operator on $\mathbb{C}^4$

Ket-ket notation

(tensor products in disguise)

The standard basis for the 2-qubit quantum system is

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle$$

It will often be convenient to write this using ket-kets:

$$|0\rangle|0\rangle, \quad |0\rangle|1\rangle, \quad |1\rangle|0\rangle, \quad |1\rangle|1\rangle$$

each of these is still a single vector in $\mathbb{C}^4$

e.g. $|0\rangle|1\rangle = |01\rangle$

Key property: If $U: \mathbb{C}^2 \to \mathbb{C}^2$ is a unitary operator, then we can extend U to act on the space of ket-kets (which is $\mathbb{C}^4$)

by defining

$$U(\overbrace{|v\rangle|w\rangle}^{\text{ket-ket lives in }\mathbb{C}^4}) = (\underbrace{U|v\rangle}_{\text{ket in }\mathbb{C}^2})|w\rangle$$

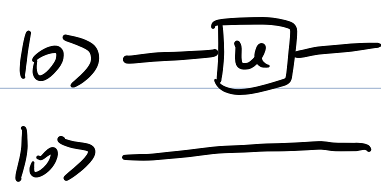
kets live in $\mathbb{C}^2$

ket in $\mathbb{C}^2$

This is called "applying U to the first ket"

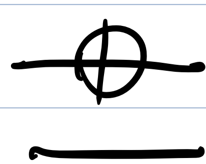
The result is a linear map $\mathbb{C}^4 \to \mathbb{C}^4$.

The notation



means "apply U to the first ket starting from the right"

e.g.

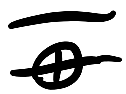


is the map $|00\rangle \mapsto |01\rangle$

$|01\rangle \mapsto |00\rangle$

$|10\rangle \mapsto |11\rangle$

$|11\rangle \mapsto |10\rangle$

similarly,  $|00\rangle \mapsto |10\rangle$

"apply $\oplus$ to the second" ket from the right

$|01\rangle \mapsto |11\rangle$

$|10\rangle \mapsto |00\rangle$

$|11\rangle \mapsto |01\rangle$

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$

$= \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$

$|01\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$

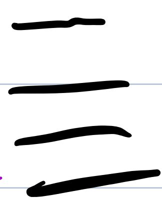
$\vdots$

q_0

q_1

q_2

q_3



$|0000\rangle$

$q_3 q_2 q_1 q_0$

2-qubit gates

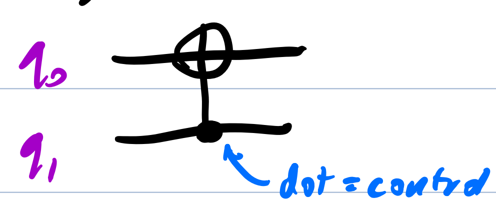
The standard examples are the

Controlled gates

For instance, the CX or CNOT gate performs the following

$$
\begin{aligned}
&\overset{q_1 q_0}{|00\rangle} \longmapsto |00\rangle \\
&|01\rangle \longmapsto |01\rangle \\
&|10\rangle \longmapsto |11\rangle \\
&|11\rangle \longmapsto |10\rangle
\end{aligned}
$$

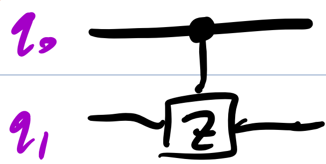
This gate is denoted



Read this as: If $q_1 = 1$ then flip q_0 (apply X to q_0)

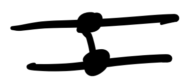
We say that q_1 is the **control** for the gate X on q_0

e.g



$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|\overset{q_1}{1}\overset{q_0}{0}\rangle \mapsto |10\rangle$$
$$|11\rangle \mapsto -|11\rangle$$

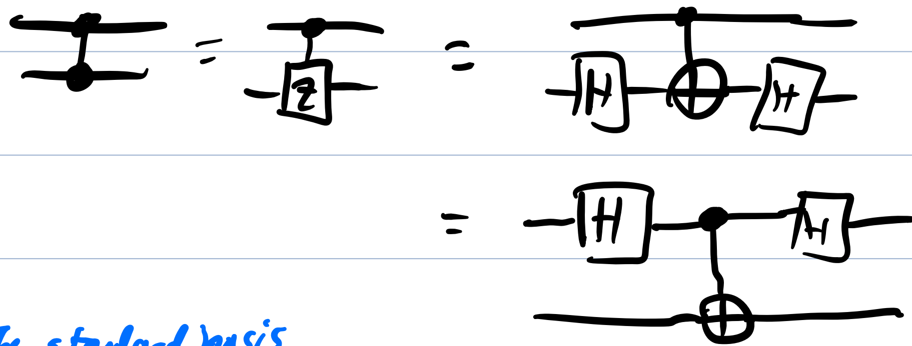
This is the CZ gate,

which is often denoted 

Expressing CZ in terms of H, CX:

Recall that $Z = HXH$, which means that "X is the Z gate in the Hadamard basis"

$\rightarrow$ "CX is the CZ gate in the Hadamard basis"



in the standard basis,

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

in the Hadamard basis

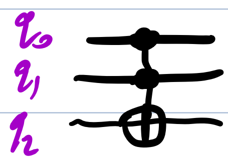
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,

$$X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Thm: Any unitary operator on a quantum computer can be built out of 1-qubit quantum gates and CNOTs.

3-qubit gates:

We can put a control on a 2-qubit gate. The standard example is the Toffoli gate (or CCX or CCNot)



flip q_2 if both $q_0 = 1$ and $q_1 = 1$.

By the Thm, a Toffoli gate can be built out of CNOTs and 1-qubit gates (though this is nontrivial)

Now lets show an application where quantum computing gives us an advantage over classical computing.

Let's say we have a function

$$f: \{0, \ldots, N-1\} \longrightarrow \{0,1\}$$

such that there is a unique ω such that $f(\omega) = 1$.

Problem: Write an algorithm to find ω given f.

E.g. Solutions to a sudoku, finding a prime factor of a composite number

Classically, we would need to call f $N-1$ times to be sure we have found ω. If we only want a 50% chance of finding ω, then we would need to call f $\frac{N}{2}$ times.

Always need $\mathcal{O}(N)$ calls to f to get to ω.

But with a quantum algorithm, we can get a 50% chance of finding ω using only $\mathcal{O}(\sqrt{N})$ calls to f.

big-$\mathcal{O}$ notation

a quantity $Q(N)$ is said to be $\mathcal{O}(\phi(N))$ if $\exists N_0, C>0$ st $\forall N \geq N_0$

$$Q(N) \leq C\,\phi(N)$$

"as $N \to \infty$ $Q(N)$ is bounded by / approx $\phi(N)$"

Next time: Grover's Algorithm