* EPR and Bell's theorem :

The phenomenon of entanglement confused many physicists at the beginning of the 20th century. It seems that measuring one qubit has an immediate action on the 2nd

$\Rightarrow$ " Spooky action at a distance " (Einstein)

which troubled many physicists in the 1930's because it was incompatible with the classical principle of locality : action a qubit A cannot influence far away qubit B (seems that this would break causality - in fact it does not ("no communication" theorem - see later))

Additionally physicists rejected the idea that measurements were probabilistic -

Classical : systems / objects have phys. prop that exist whether or not we measure / observe them.

Quantum : an unobserved particle does not possess phys. prop that exist indep of observation. Rather, such physical prop arise as a consequence of measurements performed on the system.

ex: a qubit does not possess definite spin in $\hat{z}$ direction (or $\hat{x}$ direction ...)
Rather this is revealed by doing appropriate measurement, and the outcome is probabilistic

Unless the syst is in eigenstate of the observable measured, we never know with certainty the outcome — we cannot predict it.

This view of nature was rejected by (in particular) Einstein – Podolsky – Rosen (EPR) –

They believed that the underlying physical prop. of a system exist independently of being observed –

→ this is called realism

ie they believed that it must be possible to predict with certainty the value of the property under study, immediately before the measurement.

ie there must be an "element of reality" or "hidden variable" that determine the outcome of a measurem^t.

Thus they wanted to show that QM was an incomplete theory of nature because it did not include such elements of reality.

They published a paper in 1935 to identify such elements of reality.

But they were later disproven (1964) by Bell who proposed an experiment that could check whether or not EPR was correct, and the experiment invalidated their view.

There are now many variations of Bell's proposed experiment.

Here we discuss an experiment involving 3 qubits (Mermin 1990).

Consider that someone (say David) is in possession of 3 qubits.

David prepares the 3-qubit system in an entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle - |111\rangle \right)$$

[Such 3-qubit state is called GHZ state]

David now sends a qubit each to Alice, Bob and Charlie who are all very far away from each other.

Let's consider global measurements involving $\hat{x}$ & Y operators.

We note that $|\psi\rangle$ is an eigenstate of 3-qubit operators involving 2 Y operators and 1 X operator, with eigenvalue $+1$.

For ex: $(X_A \otimes Y_B \otimes Y_C)\,|\psi\rangle$

$$= \frac{1}{\sqrt{2}}\left[X|0\rangle\, Y|0\rangle\, Y|0\rangle - X|1\rangle\, Y|1\rangle\, Y|1\rangle \right]$$

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

$$= \frac{1}{\sqrt{2}}\left[-|111\rangle + |000\rangle \right]$$

$$= +|\psi\rangle \qquad (a)$$

Same for $Y_A \otimes X_B \otimes Y_C$, $Y_A \otimes Y_B \otimes X_C$.

⇒ outcome of the measurement of these 3 observables should always be $+1$.

Now we also have

$$X_A \otimes X_B \otimes X_C\,|\psi\rangle =$$

$$= \frac{1}{\sqrt{2}}\left(X\otimes X\otimes X\,|000\rangle - X\otimes X\otimes X\,|111\rangle \right)$$

$$= \frac{1}{\sqrt{2}}\left(|111\rangle - |000\rangle \right)$$

$$= -|\psi\rangle. \qquad (b)$$

⇒ measuring $X \otimes X \otimes X$ will lead to outcome -1 with certainty.

Now if we assume local realism, as argued by EPR, there must exist a hidden variable ("element of reality") that determines the result of the measurement at each site.

For example one would have

$$\hat{X}_i \, |\psi\rangle = \eta_i^{(x)} \, |\psi\rangle \qquad i = A, B, C$$

$$\hat{Y}_i \, |\psi\rangle = \eta_i^{(y)} \, |\psi\rangle$$

So that when we measure

(i) $X_A \otimes Y_B \otimes Y_C \, |\psi\rangle = \eta_A^{(x)} \, \eta_B^{(y)} \, \eta_C^{(y)} \, |\psi\rangle$

$= + |\psi\rangle$ (from (a))

Similarly

(ii) $Y_A \otimes X_B \otimes Y_C \, |\psi\rangle = \eta_A^{(y)} \, \eta_B^{(x)} \, \eta_C^{(y)} \, |\psi\rangle = + |\psi\rangle$

(iii) $Y_A \otimes Y_B \otimes X_C \, |\psi\rangle = \eta_A^{(y)} \, \eta_B^{(y)} \, \eta_C^{(x)} \, |\psi\rangle = + |\psi\rangle$

We also have

(iv) $X_A \otimes X_B \otimes X_C \, |\psi\rangle = \eta_A^{(x)} \, \eta_B^{(x)} \, \eta_C^{(x)} \, |\psi\rangle$

$= - |\psi\rangle$ (from (b))

But (i), (ii) and (iii) lead to:

$$\eta_A^{(x)}\,\eta_B^{(x)}\,\eta_C^{(x)} = \left[\eta_A^{(y)}\,\eta_B^{(y)}\,\eta_C^{(y)}\right]^2 > 0$$

which is in contradiction with (iv).

In Nielsen and Chuang book → example for a 2-qubit Bell state:
local realism ⇒ "Bell inequalities" which are violated by QM and experiment.

→ What can we learn from this?

Entanglement is a fundamentally new set of correlations between quantum systems that do not exist classically.

In classical physics, information that enters a sub-system can be extracted from the values of the measurements while for q. systems the quantum information resides in the correlations btw the subsystems.

These correlations have physical consequences on the outputs of experiments that are beyond those obtainable from classical physics alone.

We see that having entanglement into a system opens up a new range of possibilities that are not imaginable with classical information.

The questions now are:
How much info is in these correlations?
How much can we extract from potential measurements? How can that be processed (using entanglement), and transmitted to quantum systems?
→ This is the area of **Quantum Information Science**.

How can we exploit this new resource to solve pbs that are much more difficult or even impossible with classical computers (see examples in the course – for instance simulation of quantum many body systems).

A - II) Quantum Circuits

① Basics of the circuit model.

Quantum Circuit model =
analogous of the circuit model
of classical computation.

* Classical circuits:

A deterministic classical computer evaluates a function: given n bits of input it produces m bits of output, that are uniquely determined by the input:

$$f: \{0,1\}^n \longmapsto \{0,1\}^m$$

A fct with an m-bit output is equivalat to m fcts, each with a one-bit output

$$f_1: \{0,1\}^n \longmapsto \{0,1\} = \text{first bit of the m-bit string output}$$
$$\vdots$$
$$f_m: \{0,1\}^n \longmapsto \{0,1\} = m^{th} \text{ bit}$$

=> can say that the basic task performed by a classical computer is the evaluation of functions mapping

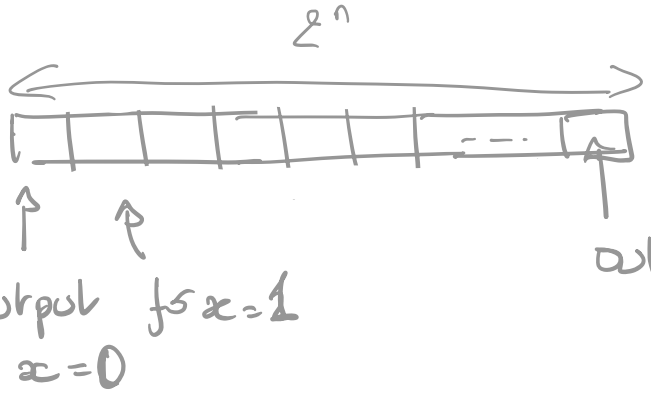
$$\{0,1\}^n \longmapsto \{0,1\}$$

= "Boolean function"

* input = n-bit string $\equiv x$ → 2^n possible inputs.

output = 1 bit

Boolean f can be seen as some array (bit-string of length 2^n)



→ How many of such fct?

= number of bit strings of size 2^n

$= 2^{2^n}$

ex: $n = 5 \rightarrow 2^{2^5} = 2^{32} > 10^9$.

(super-expo scaling).

* Another way of thinking about Boolean f

separates the n-bit strings into 2 complementary sets, the ones that it maps to 0 (rejects) & the ones that it maps to 1. (accepts)

$$\Sigma_f = \{ x \in \{0,1\}^n \mid f(x) = 1 \}$$

$$\overline{\Sigma_f} = \{ x \in \{0,1\}^n \mid f(x) = 0 \}$$

Any Boolean fct can be decomposed into simple logical operations such as NOT, AND, OR ...

NOT : $0 \mapsto 1$
$1 \mapsto 0$.

AND : $11 \mapsto 1$
$01, 10, 00 \mapsto 0$

OR : $01, 10, 11 \mapsto 1$
$00 \mapsto 0$

=> A classical computation can then be reduced to a finite sequence of such operations, applied to a specified string of input bits.

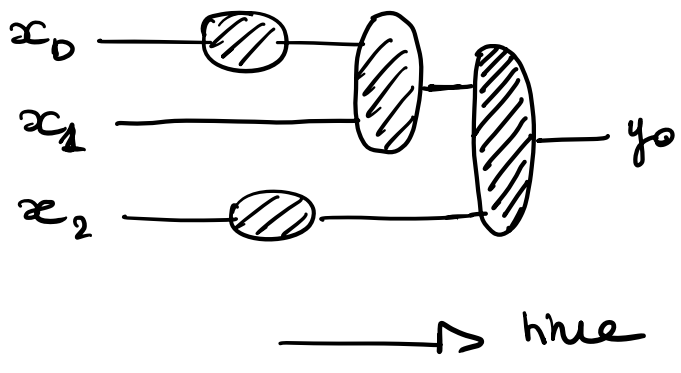
Each operation is called a **gate**.

The full sequence of operations is called **circuit**.

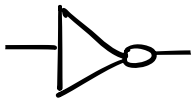
A circuit can be regarded as a **directed (acyclic) graph**, where each vertex of the graph is a gate, and the flow of bits through the circuit is indicated by directed wires.

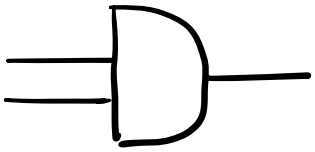
(Acyclic = no directed closed loops are permitted)

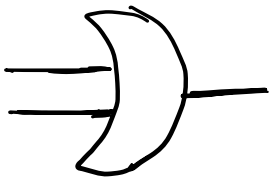
Schematically:



In practice, gates are represented by specific symbols - for example:

NOT: 

AND: 

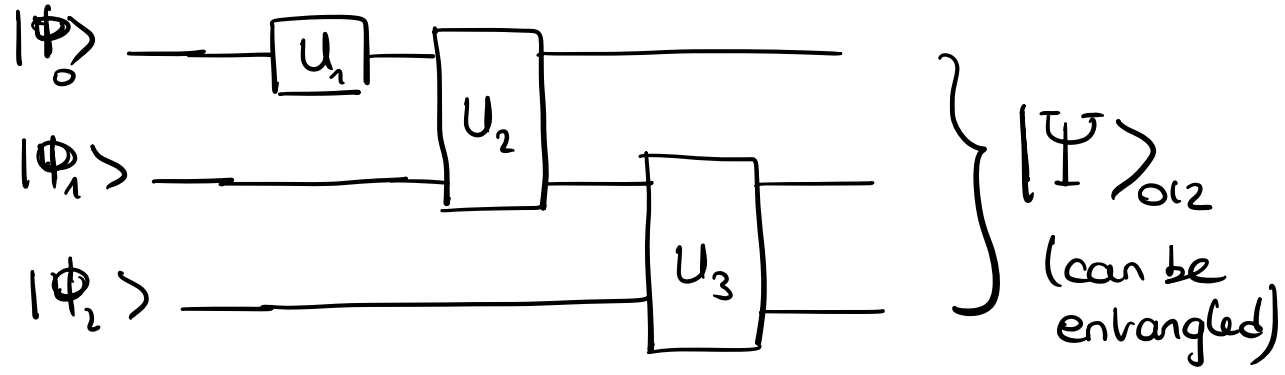
OR: 

* Quantum Circuits

A quantum circuit generalizes the idea of classical circuit to quantum computation

(The wires now represent qubits
The gates are now unitary transformations of the qubits.

Schematically:



By convention time (info) flows from left to right.

In practice the initial qubits are typically all initialized to $|0\rangle$

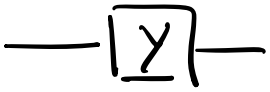
$\Rightarrow$ initial N-qubit state $= |00\ldots0\rangle \equiv |0\rangle^{\otimes N}$

We already encountered some common quantum gates in the previous section.

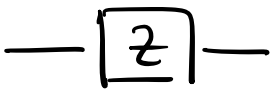
Their circuit symbols are:

X (NOT)

Y

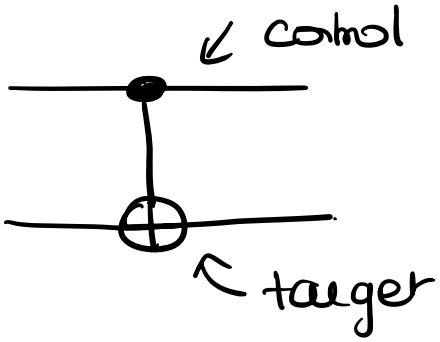


Z

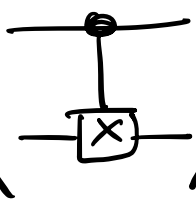


H

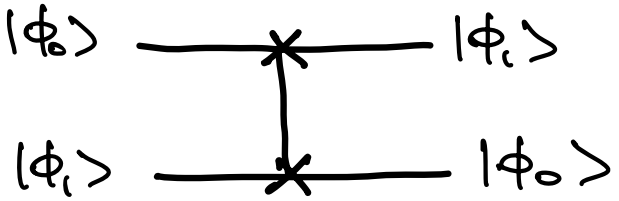
CNOT (CX)



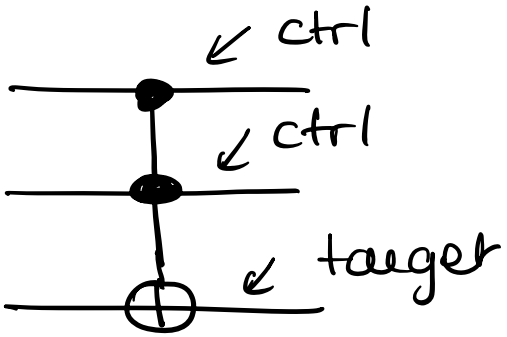
also



SWAP



CCNOT (Toffoli) (CX)



⚠ We will use the conventions of Qiskit:

A N-qubit state $|\phi_{N-1}\ \phi_{N-2} \cdots \phi_1\ \phi_0\rangle$

(ϕ_{N-1}: bottom, ϕ_0: top.)

is represented on the circuit

$|\phi_0\rangle$ ——

$|\phi_1\rangle$ ——

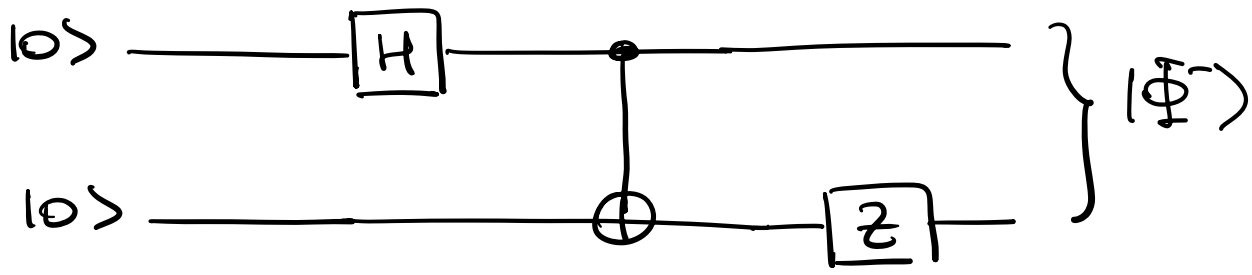
⋮

$|\phi_{N-2}\rangle$ ——

$|\phi_{N-1}\rangle$ ——

Example:

Circuit that prepares an entangled Bell state $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$



$|00\rangle \xrightarrow{H} |0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$

bottom top

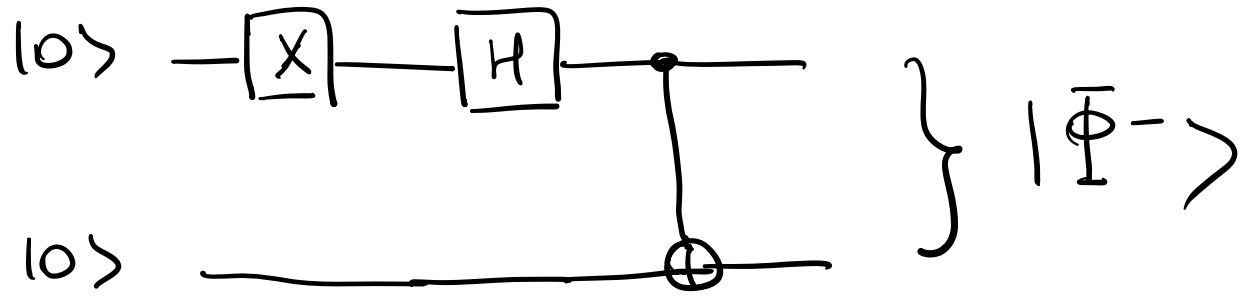
$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^{+}\rangle$

$\xrightarrow{Z} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

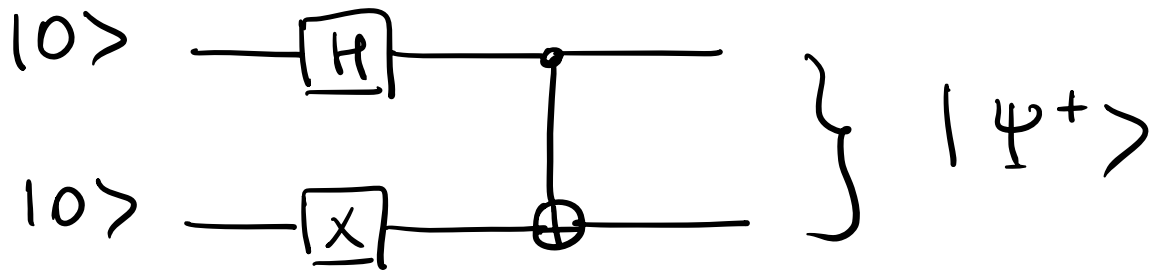
$= |\Phi^{-}\rangle$

Note that circuits are not unique

For example



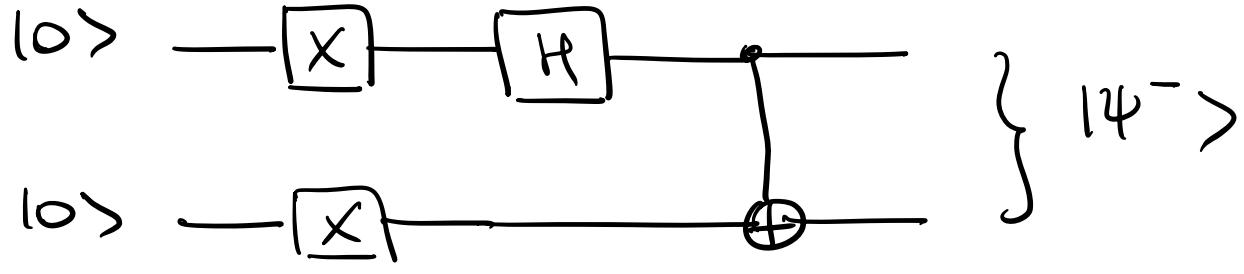
- circuits for preparing other Bell states:



$$|00\rangle \xrightarrow{X} |10\rangle \xrightarrow{H} |1+\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

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

$$= |\Psi^+\rangle$$



$$|00\rangle \xrightarrow{XX} |11\rangle \xrightarrow{H} |1-\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

$$|1-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

$$= |\Psi^-\rangle$$

(x phase (-1))

Notes : • Quantum Circuits are supposed to be generalizations of classical circuits, but they only contain unitary, thus reversible, operations, while most classical gates are not reversible (AND, OR, ...) -

⇒ not a priori obvious that QC is a generalization of CC, i.e. that any classical computation can be done with a QC - However, it turns out that any classical gate can be build from unitary operations, i.e. quantum gates (see tutorial # 2).

• Quantum comput° can also be simulated by randomized classical computers but not efficiently. (this is the belief, see later).

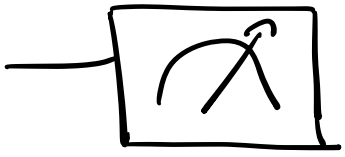
One important difference between classical and quantum computing is how to access the result of the computation.

classically → output of the computation is deterministic and extracting the output does not disturb the computation.

(deterministic computer)

quantum → accessing the result requires to measure the system — measurement are probabilistic and measuring disturbs the system. (as the system collapses to an eigenstate of the measured observable)

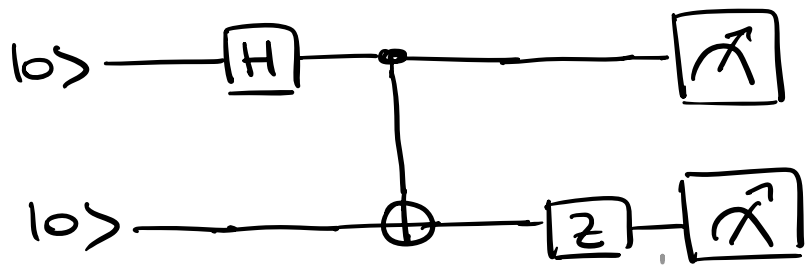
in the circuit model, measurements are represented by



In practice they are measurements along the z (observable $= \sigma_z = Z$)

↳ "measurement in the computational basis $\{|0\rangle, |1\rangle\}$."

ex



$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

⇒ after measurement the 2-qubit state collapses to

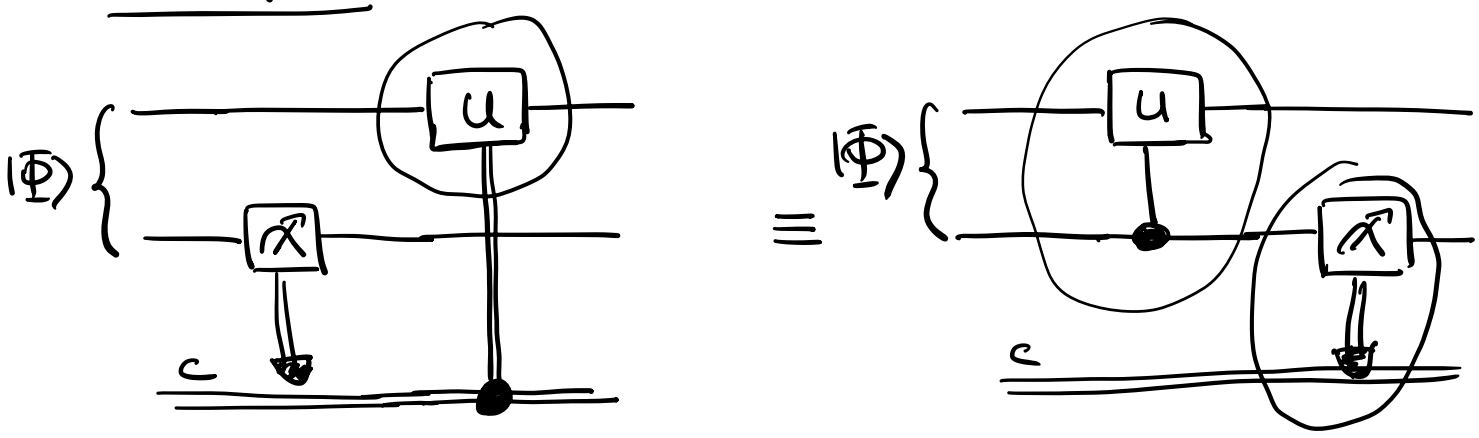
$|00\rangle$ or $|11\rangle$ each with 50% proba.

In this example, the measurement is done at the end of the computation but sometimes they can be performed as intermediate steps in the circuit and the results of the measurements are used to conditionally control subsequent quantum gates.

However it turns out that measurements can always be moved from an intermediate stage to the end of the circuit

⇒ if the measurement results are used at any stage of the circuit then the classically-controlled operations can be replaced by conditional quantum operations.
(principle of deferred measurement)

Example :



$$|\Phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

bottom top

left circuit

- Measurement of the bottom qubit $(Z \otimes \mathbb{1})$

  ⇒ Result :

  * (+1) with proba $|a_{00}|^2 + |a_{01}|^2$

    ⇒ post-meas^t state of bottom qubit $= |0\rangle$ ⇒ $c = 0$

⇒ 2-qubit state after :

$$\frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$$

* (-1) with proba $|a_{10}|^2 + |a_{11}|^2$

$\Rightarrow$ post-m. state of bottom q $= |1\rangle$ $\Rightarrow$ $c = 1$

$\Rightarrow$ 2-qubit state after : $$\frac{a_{10}|10\rangle + a_{11}|11\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}$$

- **Controlled-U** :

  * if $c = 0$ $\rightarrow$ do nothing

  2-q state : $$\left[\frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}\right]$$

  * if $c = 1$ $\rightarrow$ apply U on top qubit

$\Rightarrow$ 2-q state : $$\left[\frac{a_{10}|1\rangle \otimes U|0\rangle + a_{11}|1\rangle \otimes U|1\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}\right]$$

Right circuit

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

- **Controlled-U** :

$$\mapsto a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|1\rangle \otimes U|0\rangle + a_{11}|1\rangle \otimes U|1\rangle$$

- **Measure bottom qubit** :

* eigval $= +1$ with proba $|a_{00}|^2 + |a_{01}|^2$

$\Downarrow$

$c = 0$

$$\Rightarrow \text{2-qubit state after} = \left[\frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}} \right]$$

* eigval $= -1$ with proba $|a_{10}|^2 + |a_{01}|^2$

$\Downarrow$

$c = 1$

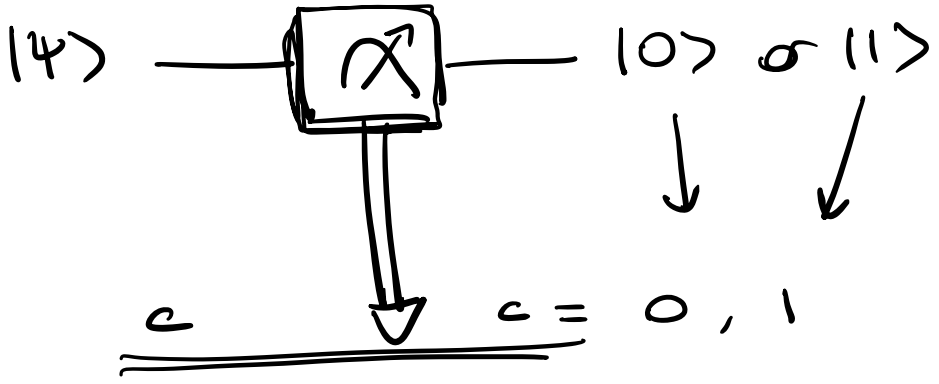
$$\Rightarrow \text{2-q state after} = \left[\frac{a_{10}|1\rangle \otimes U|0\rangle + a_{11}|1\rangle \otimes U|1\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}} \right]$$

$$= |1\rangle \otimes \left[\frac{a_{10}\, U|0\rangle + a_{11}\, U|1\rangle}{\sqrt{\quad\quad}} \right]$$

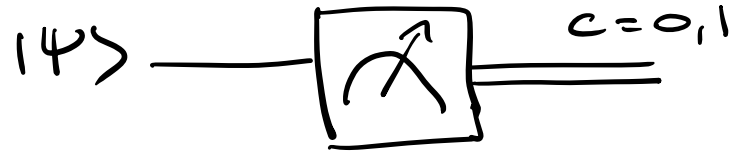
(eigenstate of $Z \otimes \mathbb{1}$.)

$\Rightarrow$ both circuits are equivalent

Note here we use the Qiskit convention



(In some textbooks (Nielsen & Chuang) this is condensed into :



)

* Measurements in other bases than the computational basis :

In practice, the measurements are done in the computational basis $\{|0\rangle, |1\rangle\}$

meaning that we measure the observable

$$\sigma_z \equiv Z = +|0\rangle\langle 0| - |1\rangle\langle 1|$$

(in general, for any observable $\hat{A}$

$$\hat{A} = \sum_n \hat{P}_n a_n$$

$\downarrow$

projectors onto eigenspace with eigenvalue a_n.

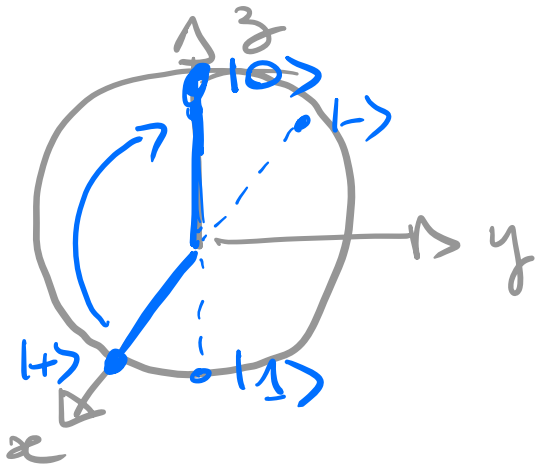
$\hat{P}_n = |n\rangle\langle n|$).

$\Rightarrow$ expectation value

$$\langle\psi|\hat{Z}|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle - \langle\psi|1\rangle\langle 1|\psi\rangle$$

Sometimes, however, we would like to measure in another basis, i.e. measure the qubit state along another axis.

This can be achieved by first "rotating" the state and then measuring along z.



(ex: $|\psi\rangle = |+\rangle \xrightarrow{\text{rotate}} |0\rangle$ and then measure along z.

$\Leftrightarrow$ measuring $|+\rangle$ along x.)

For example, say we want to measure along x $\Rightarrow$ observable is $\sigma_x \equiv X$

$$X = |+\rangle\langle+| - |-\rangle\langle-|$$

$$\text{eigenvec: } |\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$$

The transformation that takes the $\{|0\rangle, |1\rangle\}$ basis to the $(|+\rangle, |-\rangle)$ basis is the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} H = H^\dagger \\ HH^{-1} = \mathbb{1} \end{pmatrix}$$

$\Rightarrow$ can write $X = H Z H$

(can be easily checked)

$\Rightarrow$ exp. value

$$\langle\psi|X|\psi\rangle = \langle\psi|HZH|\psi\rangle$$

$$= (\langle\psi|H) \underline{Z} (\underbrace{H|\psi\rangle}_{\equiv |\psi'\rangle})$$

$= $ "rotated state"

$\Rightarrow$ measuring X is equivalent to transforming $|\psi\rangle$ and measuring Z.

Can also be seen as :

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$= \left(\frac{a+b}{\sqrt{2}}\right)|+\rangle + \left(\frac{a-b}{\sqrt{2}}\right)|-\rangle$$

→ if we could measure directly along x

$$\Rightarrow \begin{cases} +1 & \text{with proba } \left|\frac{a+b}{\sqrt{2}}\right|^2 \\ -1 & \text{with proba } \left|\frac{a-b}{\sqrt{2}}\right|^2 \end{cases}$$

→ instead : apply H :

$$H|\psi\rangle = a\,H|0\rangle + b\,H|1\rangle$$

$$= a\,|+\rangle + b\,|-\rangle$$

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

→ and measure along z :

$$\Rightarrow \begin{cases} +1 & \text{with proba } |(a+b)/\sqrt{2}|^2 \\ -1 & \text{---------- } |(a-b)/\sqrt{2}|^2 \end{cases}$$

⇒ same outcomes.

This can be done to measure in any basis - one just needs to know the transformation btw the computational basis $\{|0\rangle, |1\rangle\}$ and the eigenbasis of the observable we want to measure.

- Similarly, for multiple qubits we can measure for example $X \otimes X$ which has eigenbasis

$$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$$

= Bell state basis

the transfo U such that brings $X \otimes X$ to a diagonal form in the computational basis : eg :

$$X \otimes X = U^\dagger (Z \otimes Z) U$$

is the circuit that construct the Bell state (with CNOT & H gate)

ms circuit tutorial #3.

in fact the Bell basis is common eigenbasis of $X \otimes X$, $Y \otimes Y$, $Z \otimes Z$

(these commute, interestingly).