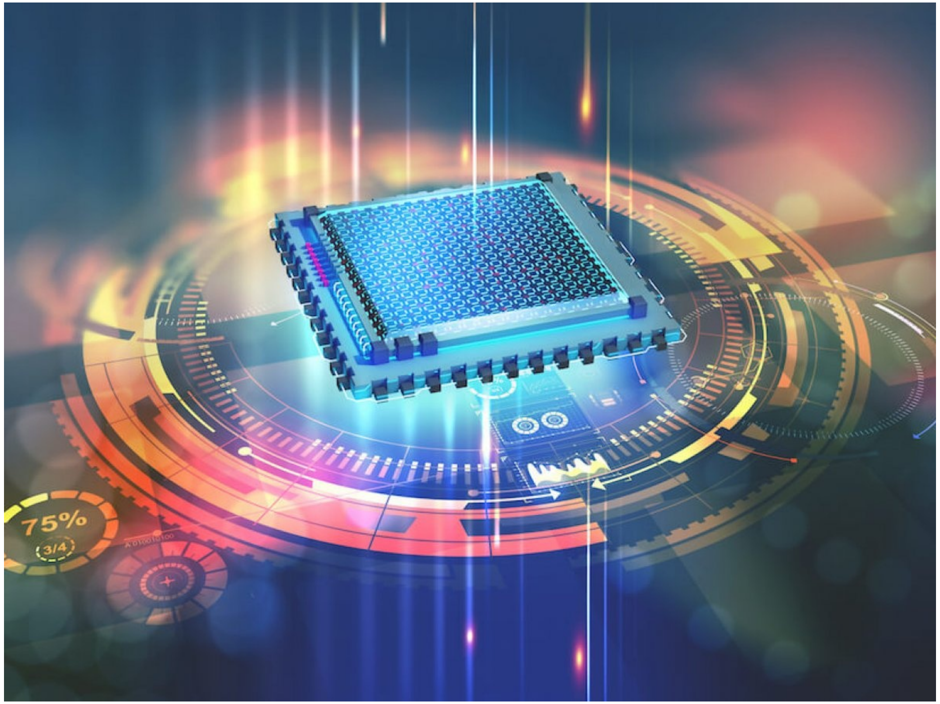
Introduction to Quantum Computing



Last class

- Two bit gates
- Quantum bits (qubits)
- A qubit is a system that obeys Axioms
  - State is a complex unit vector
  - Evolution is multiplication by unitary
  - Measurement is probabilistic, “collapses” state
  - Tensor product for combining systems

Today

- We will talk more about gates and measurements on multiple qubit systems.
- We’ll look at more examples of one and two qubit gates and what they can do. This will be useful for studying computation.

Axioms of Quantum Theory

Axiom 1 (states)

- The state of a quantum system is a complex unit vector: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, where |\alpha|^2 + |\beta|^2 = 1$
- 2-dimensional vector: qubit

  d-dimensional vector: qudit

Axioms of Quantum Theory

Axiom 2 (dynamics)

- The evolution of a closed system is described by a unitary matrix *U*

$$|\psi\rangle \text{ —— } \boxed{U} \text{ —— } U|\psi\rangle$$

Axioms of Quantum Theory

Axiom 3 (measurements)

- We can measure a system in any basis for its state space. If you measure

  $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

  in the basis $\{|0\rangle, |1\rangle\}$ the outcome is x with probability $|\alpha_x|^2$
- Furthermore, the state of the system collapses to $|x\rangle$
- This is called the Born rule

Axioms of Quantum Theory

Axiom 4 (composite systems)

If

- A has a state in span(V) for some set of vectors V
- B has a state in span(W) for some set of vectors W
- AB has a state in span($\{v \otimes w \mid v \text{ in } V, w \text{ in } W\}$)

- span(V) denotes the set of all finite linear combinations of the elements of V, $\otimes$ is the tensor product

Tensor products

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix}$$

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle = \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}$$

$$\begin{aligned}&|\psi\rangle \otimes |\phi\rangle = \\ &\quad = \alpha_0\beta_0|0\rangle\otimes|0\rangle + \alpha_0\beta_1|0\rangle\otimes|1\rangle + \alpha_1\beta_0|1\rangle\otimes|0\rangle + \alpha_1\beta_1|1\rangle\otimes|1\rangle = \\ &\quad = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\end{aligned}$$

$$\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}$$

Tensor products

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle = \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$$

First entry of
first vector

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \alpha_1 \beta_0 \\ \alpha_1 \beta_1 \end{bmatrix}$$

Two copies of the 2nd vector

Second entry of
first vector

Exercise on tensor products

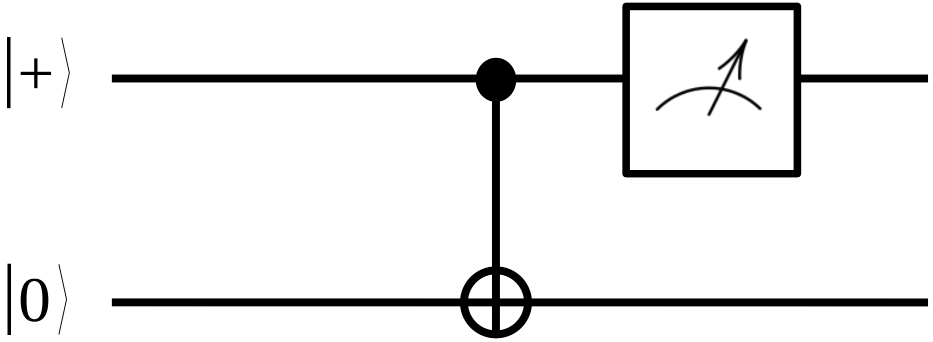
- Compute $|\psi\rangle = |+\rangle \otimes |0\rangle$
- Remember that $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- This is the state of a system made of two qubits, one in state $|+\rangle$ and one in state $|0\rangle$

Solution of the exercise

$$|\psi\rangle = |+\rangle \otimes |0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} 1 \\ \frac{1}{\sqrt{2}} 0 \\ \frac{1}{\sqrt{2}} 1 \\ \frac{1}{\sqrt{2}} 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$$

More on measurement

- What if I have multiple qubits, and I measure only one of them?



- Let’s refine axiom 3 to cover this case as well

State of n qubit system

- Any state of n qubits can be written as

  $$|\psi\rangle = \alpha_0 |0\rangle \otimes |\psi_0\rangle + \alpha_1 |1\rangle \otimes |\psi_1\rangle$$

- Where $|\psi_i\rangle$ are n-1 qubit states and

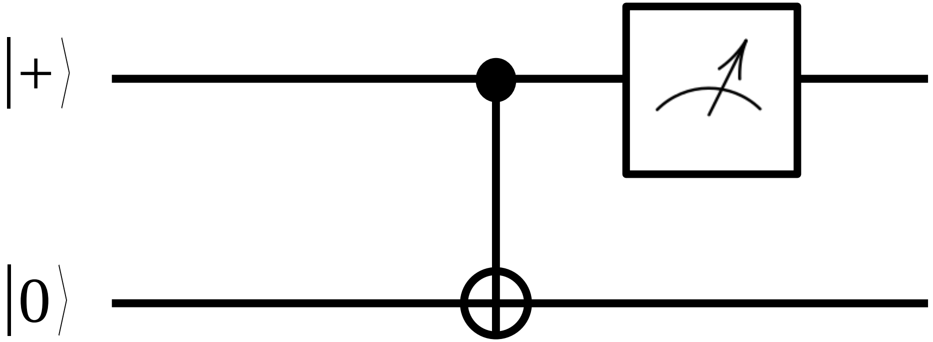
  $$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

Axioms of Quantum Theory

Axiom 3' (partial measurement)

- We can measure the first qubit of the n qubit state
  $|\psi\rangle = \alpha_0 |0\rangle \otimes |\psi_0\rangle + \alpha_1 |1\rangle \otimes |\psi_1\rangle$
  in the basis $\{|0\rangle, |1\rangle\}$.
- The outcome is x with probability $|\alpha_x|^2$
- Furthermore, the state of the system collapses to $|x\rangle \otimes |\psi_x\rangle$
- (Generalized) Born rule

So what happens here?



- We can compute the initial composite state
- We can compute the result after the CNOT
- We can compute the effect of the partial measurement (difficult using vectors, much better with kets)

Arbitrary one qubit states

- We want to prepare an arbitrary qubit state $|\psi\rangle$ starting from $|0\rangle$ (or $|1\rangle$)
- That is, we want a unitary U such that $|\psi\rangle = U|0\rangle$
- We can always find such a unitary

Finding U

- Take $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- From $|\psi\rangle = U|0\rangle$ we get

  $$U = \begin{bmatrix} \alpha & x \\ \beta & y \end{bmatrix}$$

  for some x,y
- U needs to be unitary

Finding U

- We show that $U = \begin{bmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{bmatrix}$ is unitary hence it is a solution

$$U U^\dagger = \begin{bmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \\ -\beta & \alpha \end{bmatrix} = \begin{bmatrix} \alpha \alpha^* + \beta^* \beta & \alpha \beta^* - \beta^* \alpha \\ \beta \alpha^* - \alpha^* \beta & \beta^* \beta + \alpha^* \alpha \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

How to get the $|0\rangle$

- We have learned how to get any 1 qubit state from $|0\rangle$
- We will show how to get also two qubits states
- But how to get the $|0\rangle$ to start with?
- In some cases, it can be obtained using physical processes
  - E.g., minimal energy state, by cooling down
- Otherwise, take an unknown state, measure it so to get either $|0\rangle$ or $|1\rangle$, and negate it if it is $|1\rangle$

Arbitrary two qubit states

- Now we want to prepare an arbitrary two qubit state $|\psi\rangle$ starting from $|0\rangle$s

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- One qubit gates are not enough

$$U|0\rangle \otimes V|0\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

- To have $U|0\rangle \otimes V|0\rangle = |\psi\rangle$ we need

$$\frac{\alpha_{00}}{\alpha_{01}} = \frac{\alpha_{10}}{\alpha_{11}} = \frac{\beta_0}{\beta_1}$$ what is not true in general

Adding a single CNOT is enough

- We want to prepare:

$$|\sigma\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- First, note that

$$|\sigma\rangle = |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle$$

with $|\psi\rangle = \alpha_{00}|0\rangle + \alpha_{01}|1\rangle$ and $|\phi\rangle = \alpha_{10}|0\rangle + \alpha_{11}|1\rangle$

- We want to find U such that

$$U \otimes I|\sigma\rangle = |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$$

with $|\psi'\rangle$ and $|\phi'\rangle$ orthogonal

(if $|\psi\rangle$ and $|\phi\rangle$ are orthogonal we can choose $U = I$)

Finding U

- We want to find U such that

$$U \otimes I |\sigma\rangle = |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$$

- Let us try with

$$U = \begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix}$$ which we know is unitary

$$U \otimes I |\sigma\rangle = (a|0\rangle + b|1\rangle) \otimes |\psi\rangle + (-b^*|0\rangle + a^*|1\rangle) \otimes |\phi\rangle =$$
$$= |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$$
$$\text{where } |\psi'\rangle = a|\psi\rangle - b^*|\phi\rangle \text{ and } |\phi'\rangle = b|\psi\rangle + a^*|\phi\rangle$$

Orthogonal vectors

- Two vectors $|\psi\rangle, |\phi\rangle$ are orthogonal iff $\langle\psi|\phi\rangle = 0$
- This is the inner product
- Namely $\sum_{i=1}^{n} \psi_i^* \phi_i$
- Note that $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$
- It is linear in the right argument, antilinear in the left one
- Inner product of a unitary vector for itself is 1

Computing the coefficients

- We want

  $|\phi'\rangle = b|\psi\rangle + a^*|\phi\rangle$ and $|\psi'\rangle = a|\psi\rangle - b^*|\phi\rangle$

  orthogonal

$$0 = \langle\phi'|\psi'\rangle = b^* a\langle\psi|\psi\rangle + aa\langle\phi|\psi\rangle - b^* b^*\langle\psi|\phi\rangle - ab^*\langle\phi|\phi\rangle =$$
$$= a^2\langle\phi|\psi\rangle - b^{*2}\langle\psi|\phi\rangle + ab^*(\langle\psi|\psi\rangle - \langle\phi|\phi\rangle) =$$
$$= a^2\langle\phi|\psi\rangle - b^{*2}\langle\psi|\phi\rangle$$

- We can solve the equation to derive values for a and b

Normalization

- We have
  $U \otimes I|\sigma\rangle = |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$
  with $|\psi'\rangle$ and $|\phi'\rangle$ orthogonal

- They may not be normalized yet, we need to divide them for their module, hence we define

  $$|\psi''\rangle = \frac{|\psi'\rangle}{\lambda}, |\phi''\rangle = \frac{|\phi'\rangle}{\mu}$$

- They are still orthogonal and now unitary

Tensor product of matrices

- We want
  $$(U \otimes V)(|\phi\rangle \otimes |\psi\rangle) = U|\phi\rangle \otimes V|\psi\rangle$$
- We can actually define it as follows:

$$U = \begin{bmatrix} u_{1,1} & u_{1,2} \\ u_{2,1} & u_{2,2} \end{bmatrix} \qquad V = \begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix}$$

$$U \otimes V = \begin{bmatrix} u_{1,1}\begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix} & u_{1,2}\begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix} \\ u_{2,1}\begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix} & u_{2,2}\begin{bmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} u_{1,1}v_{1,1} & u_{1,1}v_{1,2} & u_{1,2}v_{1,1} & u_{1,2}v_{1,2} \\ u_{1,1}v_{2,1} & u_{1,1}v_{2,2} & u_{1,2}v_{2,1} & u_{1,2}v_{2,2} \\ u_{2,1}v_{1,1} & u_{2,1}v_{1,2} & u_{2,2}v_{1,1} & u_{2,2}v_{1,2} \\ u_{2,1}v_{2,1} & u_{2,1}v_{2,2} & u_{2,2}v_{2,1} & u_{2,2}v_{2,2} \end{bmatrix}$$

Building the circuit (1)

- Take V (unitary) such that
  $|\psi''\rangle = V|0\rangle, |\phi''\rangle = V|1\rangle$

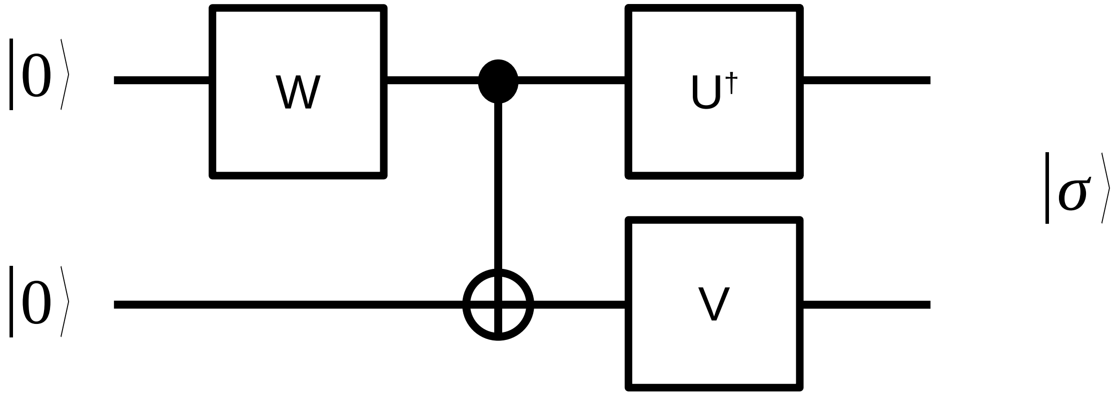
- We have

$$U \otimes I|\sigma\rangle = |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle$$
$$U \otimes I|\sigma\rangle = |0\rangle \otimes \lambda|\psi''\rangle + |1\rangle \otimes \mu|\phi''\rangle$$
$$U \otimes I|\sigma\rangle = |0\rangle \otimes \lambda V|0\rangle + |1\rangle \otimes \mu V|1\rangle$$
$$U \otimes I|\sigma\rangle = (I \otimes V)(\lambda|0\rangle \otimes |0\rangle + \mu|1\rangle \otimes |1\rangle)$$
$$|\sigma\rangle = (U^\dagger \otimes V)(\lambda|0\rangle \otimes |0\rangle + \mu|1\rangle \otimes |1\rangle)$$

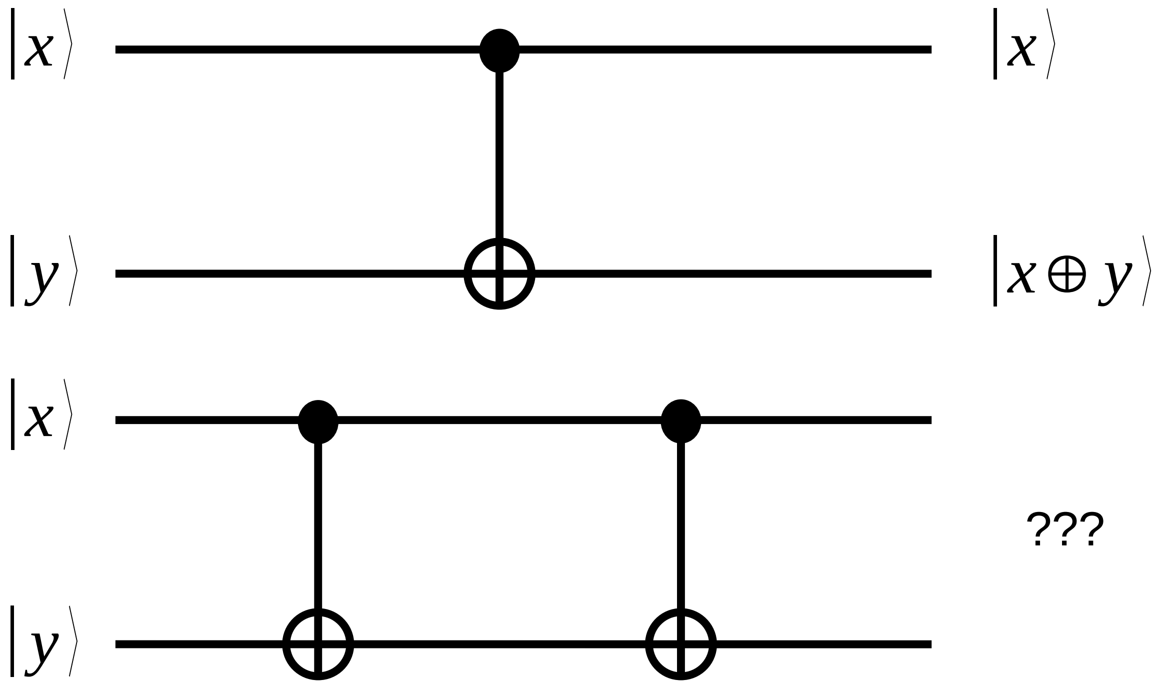
Building the circuit (2)

- $$|\sigma\rangle = (U^\dagger \otimes V)(\lambda|0\rangle \otimes |0\rangle + \mu|1\rangle \otimes |1\rangle) =$$
  $$= (U^\dagger \otimes V)\,CNOT((\lambda|0\rangle + \mu|1\rangle) \otimes |0\rangle) =$$
  $$= (U^\dagger \otimes V)\,CNOT((W|0\rangle) \otimes |0\rangle)$$

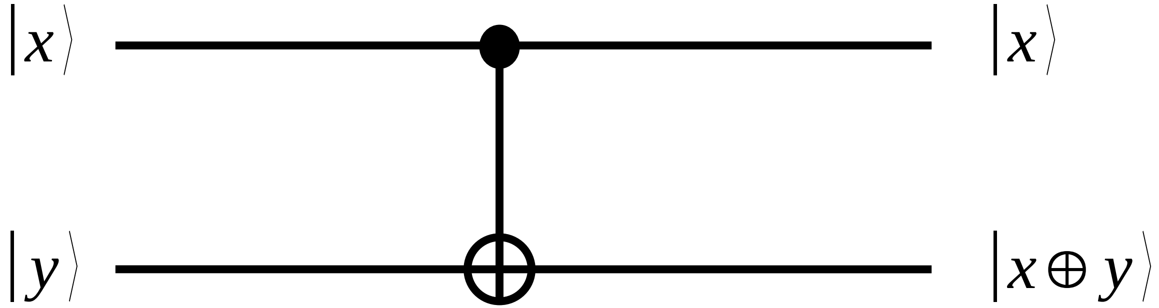
  for some W unitary

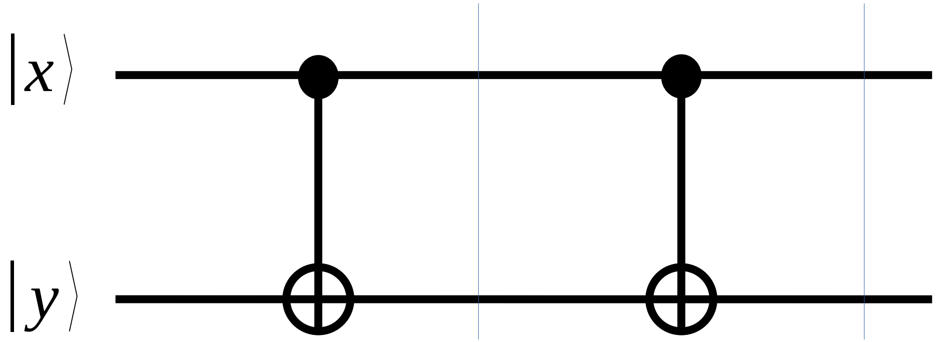


More on CNOT



More on CNOT



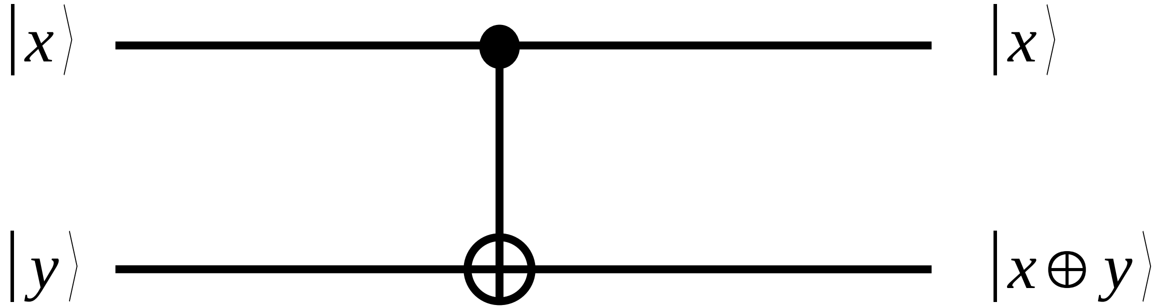


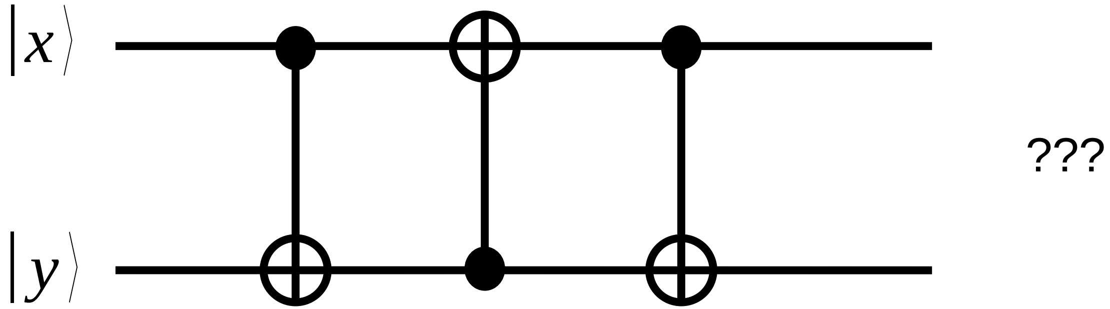
???

State here is
$|x\rangle|x \oplus y\rangle$

State here is
$|x\rangle|x \oplus (x \oplus y)\rangle = |x\rangle|y\rangle$

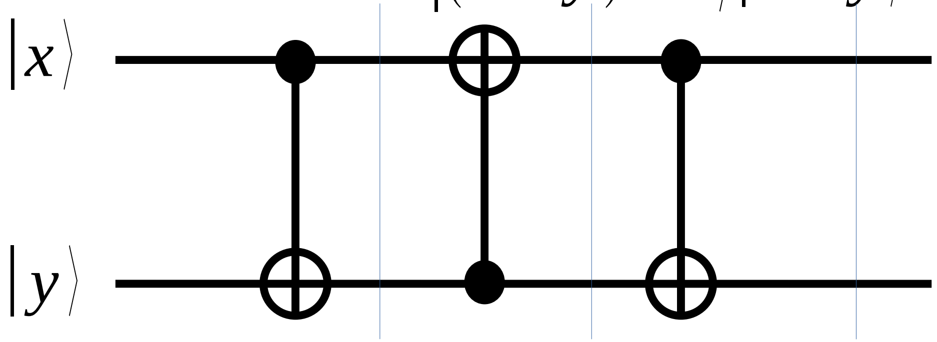
CNOT exercise





CNOT exercise

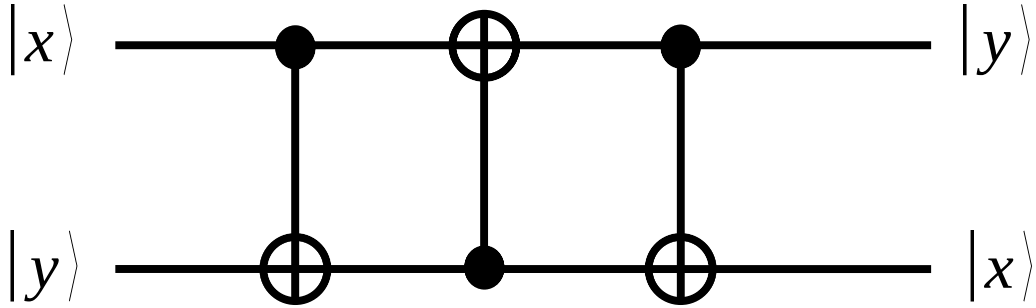
State here is
$$\left|(x\oplus y)\oplus x\right\rangle\left|x\oplus y\right\rangle=\left|y\right\rangle\left|x\oplus y\right\rangle$$



State here is
$$\left|x\right\rangle\left|x\oplus y\right\rangle$$

State here is
$$\left|y\right\rangle\left|y\oplus(x\oplus y)\right\rangle=\left|y\right\rangle\left|x\right\rangle$$

CNOT exercise



- This is actually a swap

Summary

- Tensor products of vectors (to compose states) and of matrices (to compose circuits)
- I can prepare an arbitrary 1 qubit state with a 1 qubit unitary
- For 2 qubits states I need CNOT (and 3 unitaries)