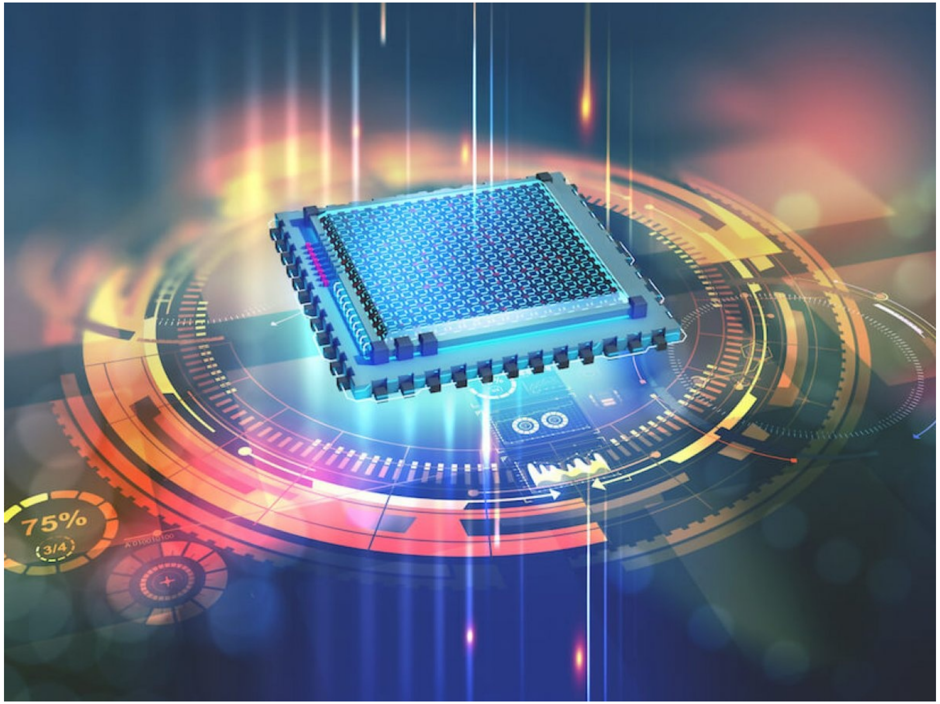
Introduction to Quantum Computing



Reversible classical circuits

- We have seen some classical operations on bits
  - NOT, swap, CNOT
- You can create classical circuits composing them
- Actually, classical *reversible* circuits
  - Circuits where you can as well compute input from output
  - The circuits above are self-inverse: if you compose two copies of them you get the identity

From classical to quantum

- Now you could study classical (reversible) computation
- Figure out which gates you need to do stuff, how many of them …
- We will not do this
- We will move from classical computation to quantum computation
- Our model will be based on qubits, not on bits
- Qubits extend bits, and allow for quantum effects

What is a qubit?

- A **quantum** system whose state is a 2-dimensional complex unit vector, namely:

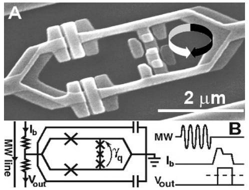
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \textit{where}\, |\alpha|^2 + |\beta|^2 = 1$$

- 2-dimensional vector: linear combination of 2 linearly independent elements (base)
- Complex: α and β are complex numbers
- Unit: the length of the vector is 1, as captured by the side condition, where if α=a+ib then $|\alpha| = \sqrt{a^2 + b^2}$

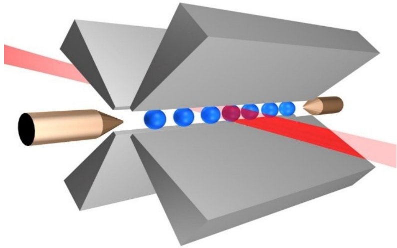
Bits as qubits

- A classical bit is just a qubit, which also satisfies $\alpha = 1$ or $\beta = 1$
- Actually, all bits are really qubits.
- But for most systems we are used to, natural physical processes drive an arbitrary state $|\psi\rangle$ to either $|1\rangle$ or $|0\rangle$ really fast. So it's hard to see the quantumness.

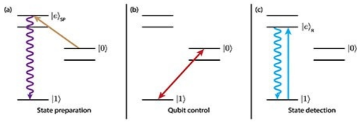
What is a qubit?

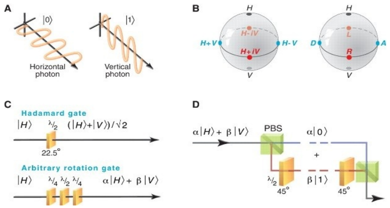


Superconducting circuits

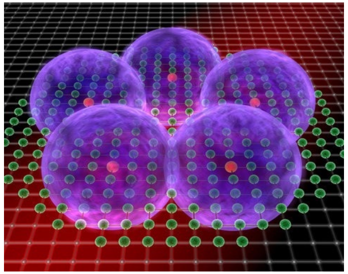


Ion traps





Polarization of a photon



Rydberg states: excited or not

A real qubit is quite complex

- It would take a whole other course (with WAY more prereqisites) to understand “which systems make good qubits?”
- For us, it’s enough to know: people are getting pretty good at making systems with 100’s of qubits right now. Plausible paths to 1,000,000’s within 10’s of years.
- Our goal is to understand the computational model that quantum theory implies, and better understand what quantum computers can do.

Levels of abstraction

- As usual in computer science, when something is too complex, we use abstraction to hide complexity
- In real life: I can use TV without knowing how it works. I just need to know what to do with the TV controller
- In programming: I can invoke a function (or a web service) without knowing its implementation, I just need to know its interface and specification

Our level of abstraction

- We are in the business of using qubits, not building them or fixing them.
- For us, a quantum system is just something whose state is a complex unit vector
- Qubits can be the polarization of a photon, two hyperfine states of an atom, etc., but you do not care
- This avoids the need for a lot of physics, and will work also on future implementations

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

- α and β are called amplitudes

Sample states

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

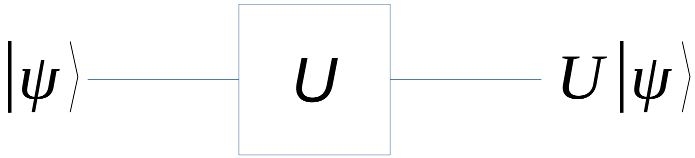
- Sort of like “50% 0, 50% 1”, but also different

  (we’ll see more later in the measurement axiom)
- These are examples of states in a *superposition* (states not in a superposition are called basis states)

Axioms of Quantum Theory

Axiom 2 (dynamics)

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



Unitary matrix

- Unitary means that $U^{\dagger} U = I$,
  where $U^{\dagger}$ is the conjugate transpose
- Transpose: swap rows and columns
- Conjugate: for each element, change the sign of the complex part
  - E.g., an element 3+2i goes to 3-2i
- A unitary matrix maps unitary vectors to unitary vectors

Four fantastic unitaries

- The identity and the 3 Pauli matrices (rotations in Bloch sphere)

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

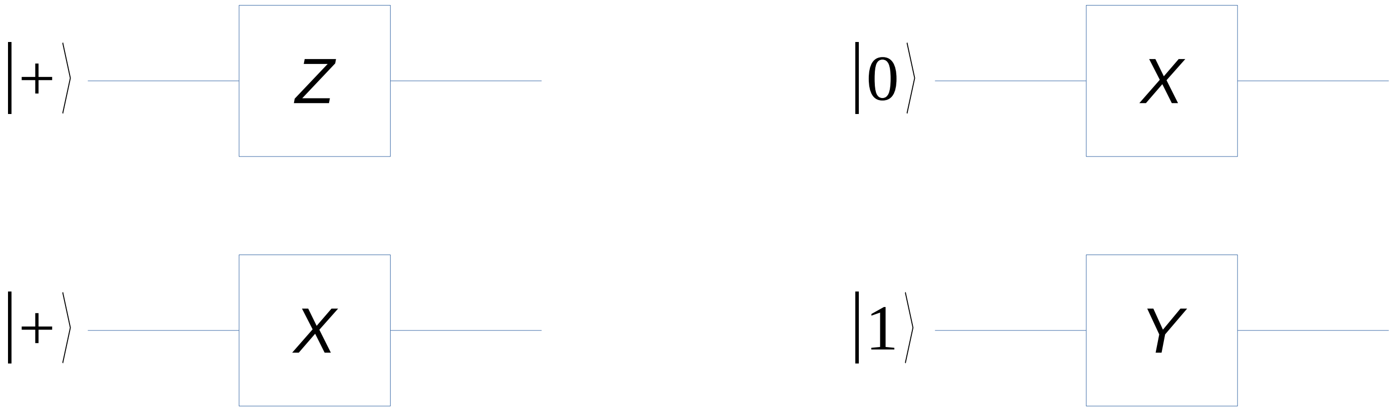
$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Check, are these unitaries?

$$Y^\dagger Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

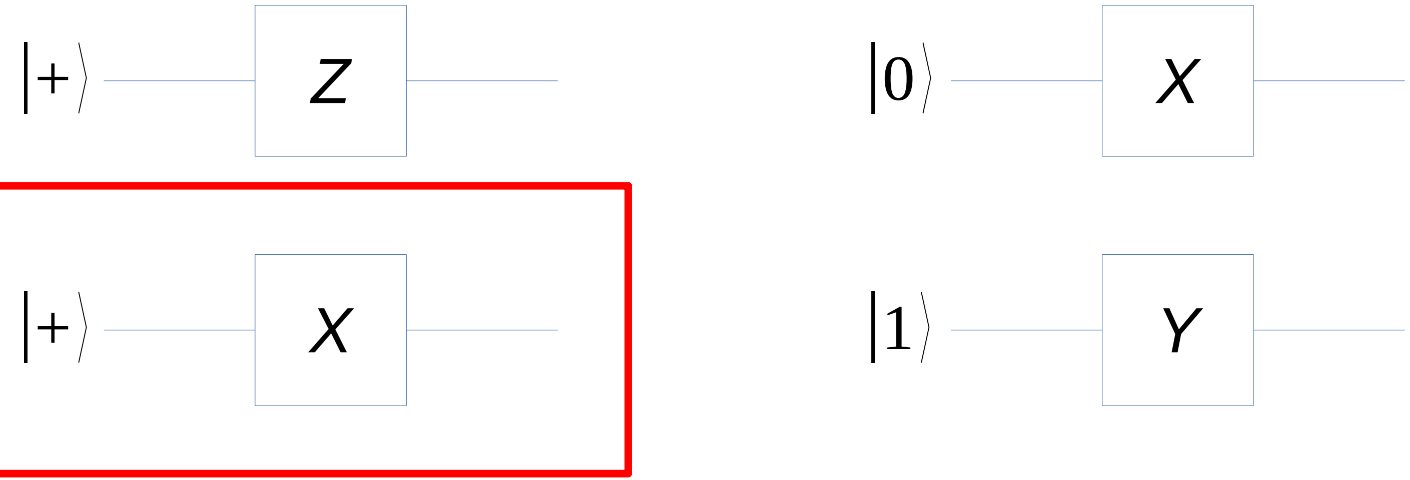
Exercise

Which circuit prepares $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$?



Exercise: solution

Which circuit prepares $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$?



The solution, proved

- We have to show $X|+\rangle = |+\rangle$
- Since X is NOT, and is linear:

$$X|+\rangle = X\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =$$

$$= \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle = |+\rangle$$

The solution, using matrices

- We have to show $X|+\rangle = |+\rangle$

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

- Slightly more complex, but works in the very same way for every operator

Hadamard

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

$H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$

- Since $H^\dagger H = I$ and $H^\dagger = H$ we also have $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$
- Very useful, we can create and destroy superpositions

So far

- Axiom 1: states are complex unit vectors
- Axiom 2: evolution is multiplication by unitary matrices
- What else?

So far

- Axiom 1: states are complex unit vectors
- Axiom 2: evolution is multiplication by unitary matrices
- What else?
- We have a theory of vectors that you can rotate. The state is a collection of complex numbers (so an infinite number of bits).
- The next axiom tells us that the information we can extract about the state of a system is very limited.

Axioms of Quantum Theory

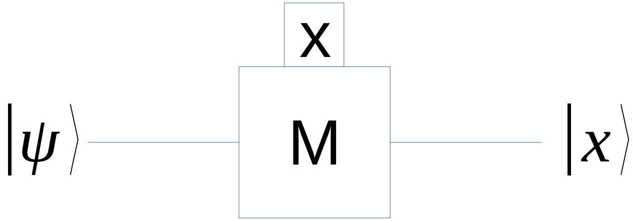
Axiom 3 (measurements)

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

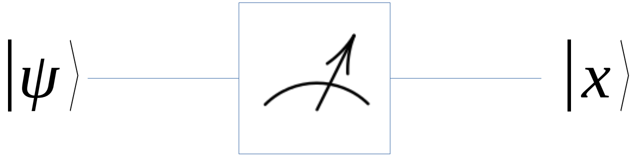
  $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

  in the basis $\{|0\rangle, |1\rangle\}$ (computational basis) the result is probabilistic
- You get an outcome x with probability $|\alpha_x|^2$
- Furthermore, the state of the system collapses to $|x\rangle$

Measurement: circuit diagram



Book notation



More common notation

Exercises

- What if you measure $|1\rangle$ in the basis $\{|+\rangle,|-\rangle\}$?
- And if then you measure the result again, in the computational basis?

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

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

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

Today

- 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