Quantum Computation and Cryptography
Day 2

Alexandru Gheorghiu

The University of Edinburgh

Part I
The basics of quantum mechanics

"*There's no royal road to geometry*" - Euclid

"*There's no royal road to geometry*" - Euclid

There's no royal road to quantum computing, either!

"*There's no royal road to geometry*" - Euclid

There's no royal road to quantum computing, either!

We're going to look at and understand the postulates of quantum mechanics

"*There's no royal road to geometry*" - Euclid

There's no royal road to quantum computing, either!

We're going to look at and understand the postulates of quantum mechanics

Quantum mechanics $\neq$ physical theory
Quantum mechanics $=$ framework for building physical theories

"*There's no royal road to geometry*" - Euclid

There's no royal road to quantum computing, either!

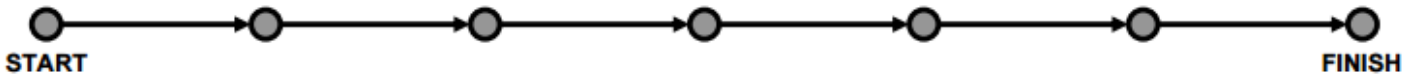
We're going to look at and understand the postulates of quantum mechanics

Quantum mechanics $\neq$ physical theory
Quantum mechanics $=$ framework for building physical theories

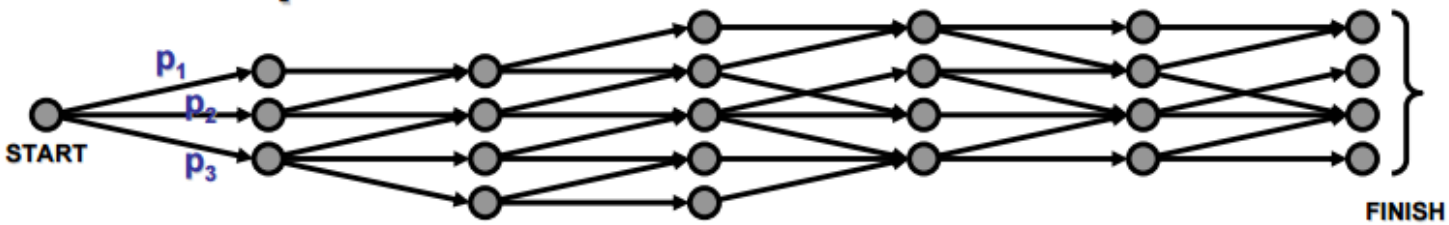
"*Quantum mechanics is actually remarkably simple, once you take all the physics out of it!*" - Scott Aaronson

Recap

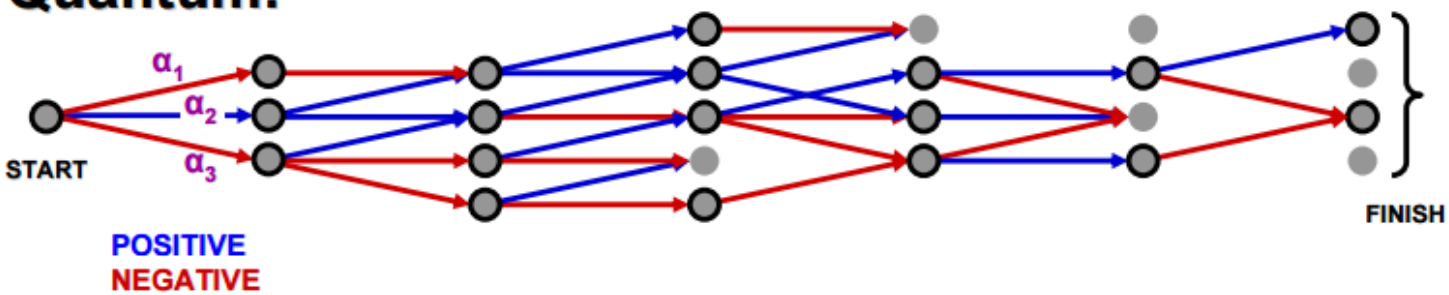
Classical deterministic:



Classical probabilistic:



Quantum:



Recap

- Computer memory is 2^N-dimensional vector

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1
- Computation achieved by applying a **unitary matrix**

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1
- Computation achieved by applying a **unitary matrix**
- Interference of computation paths

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1
- Computation achieved by applying a **unitary matrix**
- Interference of computation paths
- Output probability distribution given by Born's law

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1
- Computation achieved by applying a **unitary matrix**
- Interference of computation paths
- Output probability distribution given by Born's law
- Outcome taken according to that distribution

Recap

- Computer memory is 2^N-dimensional vector
- The vector has norm 1
- Computation achieved by applying a **unitary matrix**
- Interference of computation paths
- Output probability distribution given by Born's law
- Outcome taken according to that distribution

This is the essence of quantum mechanics!

Postulate I - state representation (intuition)

Postulate I - state representation (intuition)

The state of a system should be a norm 1 vector in a complex vector space

Postulate I - state representation

The state of an isolated quantum system is a ray of norm 1 in a complex vector space called Hilbert space.

Once upon a time in high-school

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

$\bar{z} = re^{-i\phi}$ is the **complex conjugate** of z

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

$\bar{z} = re^{-i\phi}$ is the **complex conjugate** of z

$$z\bar{z} = |z|^2 = re^{i\phi}\ re^{-i\phi} = r^2$$

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

$\bar{z} = re^{-i\phi}$ is the **complex conjugate** of z

$$z\bar{z} = |z|^2 = re^{i\phi}\ re^{-i\phi} = r^2$$

$$e^{i\phi} = cos(\phi) + i\ sin(\phi)$$

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

$\bar{z} = re^{-i\phi}$ is the **complex conjugate** of z

$$z\bar{z} = |z|^2 = re^{i\phi}\ re^{-i\phi} = r^2$$

$$e^{i\phi} = cos(\phi) + i\ sin(\phi)$$

$$v = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} r_1 e^{i\phi_1} \\ r_2 e^{i\phi_2} \end{pmatrix} = e^{i\phi_1} \begin{pmatrix} r_1 \\ r_2 e^{i\Delta\phi} \end{pmatrix}$$

Once upon a time in high-school

If $z \in \mathbb{C}$, then $z = re^{i\phi}$

r is the **magnitude**
ϕ is the **phase**

$\bar{z} = re^{-i\phi}$ is the **complex conjugate** of z

$$z\bar{z} = |z|^2 = re^{i\phi}\ re^{-i\phi} = r^2$$

$$e^{i\phi} = cos(\phi) + i\ sin(\phi)$$

$$v = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} r_1 e^{i\phi_1} \\ r_2 e^{i\phi_2} \end{pmatrix} = e^{i\phi_1} \begin{pmatrix} r_1 \\ r_2 e^{i\Delta\phi} \end{pmatrix}$$

We call ϕ_1 the **global phase** of v
And $\Delta\phi = \phi_2 - \phi_1$ the **relative phase**

Postulate I

Ray? What's a ray?

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

I.e. $\forall\, \phi$, V and $e^{i\phi} V$ are the same ray (equivalence class)

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

I.e. $\forall\, \phi$, V and $e^{i\phi} V$ are the same ray (equivalence class)

Only care about *relative phase* (we'll see an example soon)

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

I.e. $\forall\, \phi$, V and $e^{i\phi}V$ are the same ray (equivalence class)

Only care about *relative phase* (we'll see an example soon)

What's a Hilbert space? (denoted $\mathcal{H}$)

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

I.e. $\forall\ \phi$, V and $e^{i\phi}V$ are the same ray (equivalence class)

Only care about *relative phase* (we'll see an example soon)

What's a Hilbert space? (denoted $\mathcal{H}$)

- Complex or real vector space with inner product $\langle , \rangle$
- $\forall\ x, y \in \mathcal{H},\ \langle x, y \rangle \in \mathbb{C}$
- $\forall\ x, y \in \mathcal{H},\ \langle x, y \rangle = \overline{\langle y, x \rangle}$
- $\forall\ x_1, x_2, y \in \mathcal{H},\ \forall\ a, b \in \mathbb{C},$
  $\langle a x_1 + b x_2, y \rangle = a \langle x_1, y \rangle + b \langle x_2, y \rangle$
- $\forall\ x, y_1, y_2 \in \mathcal{H},\ \forall\ a, b \in \mathbb{C},$
  $\langle x, a y_1 + b y_2 \rangle = \bar{a} \langle x, y_1 \rangle + \bar{b} \langle x, y_2 \rangle$
- $\forall\ x \in \mathcal{H},\ \langle x, x \rangle \geq 0$ (define $\|x\|^2 = \langle x, x \rangle$)

Postulate I

Ray? What's a ray?

A vector for which we ignore its *global phase*

I.e. $\forall\ \phi$, V and $e^{i\phi}V$ are the same ray (equivalence class)

Only care about *relative phase* (we'll see an example soon)

What's a Hilbert space? (denoted $\mathcal{H}$)

It's a vector space with nice properties like **linearity** and **positivity**!

The qubit
Representation 1

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

M_f can act on v_R and change it to another qubit, for example...

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

M_f can act on v_R and change it to another qubit, for example...

$$M_f = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}, \; M_f v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; M_f v_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

M_f can act on v_R and change it to another qubit, for example...

$$M_f = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}, \; M_f v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; M_f v_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\text{In general, } v = \begin{pmatrix} a \\ b \end{pmatrix}, \text{ such that } |a|^2 + |b|^2 = 1$$

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

M_f can act on v_R and change it to another qubit, for example...

$$M_f = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}, \; M_f v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; M_f v_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

In general, $v = \begin{pmatrix} a \\ b \end{pmatrix}$, such that $|a|^2 + |b|^2 = 1$

Note that $v = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ i \end{pmatrix}$, and $M_f v_0$ are the same ray

The qubit
Representation 1

Say our quantum computer has $N = 1$ qubit, so $R = [R_1]$

So v_R is a 2-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

M_f can act on v_R and change it to another qubit, for example...

$$M_f = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}, \; M_f v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; M_f v_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

In general, $v = \begin{pmatrix} a \\ b \end{pmatrix}$, such that $|a|^2 + |b|^2 = 1$

Note that $v = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ i \end{pmatrix}$, and $M_f v_0$ are the same ray

But $M_f v_0$ and $M_f v_1$ are not!

The qubit
Representation 2

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

We also have $\langle\psi| = \bar{a}\,\langle 0| + \bar{b}\,\langle 1| \leftrightarrow \bar{v}^T = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

We also have $\langle\psi| = \bar{a}\,\langle 0| + \bar{b}\,\langle 1| \leftrightarrow \bar{v}^T = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$

$$\langle 0\,|\,0\rangle = \langle 1\,|\,1\rangle = \langle\psi\,|\,\psi\rangle = 1 \leftrightarrow \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

We also have $\langle\psi| = \bar{a}\,\langle 0| + \bar{b}\,\langle 1| \leftrightarrow \bar{v}^T = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$

$$\langle 0\,|\,0\rangle = \langle 1\,|\,1\rangle = \langle\psi\,|\,\psi\rangle = 1 \leftrightarrow \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

$$\langle 0\,|\,1\rangle = \langle 1\,|\,0\rangle = 0$$

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

We also have $\langle\psi| = \bar{a}\,\langle 0| + \bar{b}\,\langle 1| \leftrightarrow \bar{v}^T = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$

$$\langle 0\,|\,0\rangle = \langle 1\,|\,1\rangle = \langle\psi\,|\,\psi\rangle = 1 \leftrightarrow \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

$$\langle 0\,|\,1\rangle = \langle 1\,|\,0\rangle = 0$$

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

The qubit
Representation 2

The 0 state $|0\rangle \leftrightarrow v_0$

The 1 state $|1\rangle \leftrightarrow v_1$

Arbitrary state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \leftrightarrow v = \begin{pmatrix} a \\ b \end{pmatrix}$

where $|a|^2 + |b|^2 = 1$

We also have $\langle\psi| = \bar{a}\,\langle 0| + \bar{b}\,\langle 1| \leftrightarrow \bar{v}^T = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$

$$\langle 0\,|\,0\rangle = \langle 1\,|\,1\rangle = \langle\psi\,|\,\psi\rangle = 1 \leftrightarrow \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

$$\langle 0\,|\,1\rangle = \langle 1\,|\,0\rangle = 0$$

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

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

The qubit
Representation 2

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$
- $\langle\chi\,|\,\psi\rangle$ is the inner product

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$
- $\langle\chi\,|\,\psi\rangle$ is the inner product
- $\langle\chi\,|\,\psi\rangle = \overline{\langle\psi\,|\,\chi\rangle}$

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$
- $\langle\chi\,|\,\psi\rangle$ is the inner product
- $\langle\chi\,|\,\psi\rangle = \overline{\langle\psi\,|\,\chi\rangle}$
- The qubit lives in a 2-dimensional Hilbert space and ($|0\rangle$, $|1\rangle$) forms an orthonormal basis

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$
- $\langle\chi\,|\,\psi\rangle$ is the inner product
- $\langle\chi\,|\,\psi\rangle = \overline{\langle\psi\,|\,\chi\rangle}$
- The qubit lives in a 2-dimensional Hilbert space and ($|0\rangle$, $|1\rangle$) forms an orthonormal basis
- $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \neq v = \begin{pmatrix} a \\ b \end{pmatrix}$

The qubit
Representation 2

- $|\psi\rangle$ is called **ket psi**
- $\langle\psi|$ is called **bra psi** and is the **adjoint** of $|\psi\rangle$
- $\langle\chi\,|\,\psi\rangle$ is the inner product
- $\langle\chi\,|\,\psi\rangle = \overline{\langle\psi\,|\,\chi\rangle}$
- The qubit lives in a 2-dimensional Hilbert space and ($|0\rangle$, $|1\rangle$) forms an orthonormal basis
- $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \neq v = \begin{pmatrix} a \\ b \end{pmatrix}$
- Rather, $|\psi\rangle \leftrightarrow v$. They represent the same thing but are not equal

Superposition

Note that superposition is just linear combination of basis states!

Superposition

Note that superposition is just linear combination of basis states!

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

Superposition

Note that superposition is just linear combination of basis states!

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

$$|\text{electron path}\rangle = a_1\,|path_1\rangle + a_2\,|path_2\rangle + ...$$

Superposition

Oddly enough, politicians excel at quantum mechanics.

Postulate II - composing systems
Intuition

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ...

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ...

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ... 32-dimensional space
($|00000\rangle$, $|00001\rangle$, ... $|11111\rangle$)

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ... 32-dimensional space
($|00000\rangle$, $|00001\rangle$, ... $|11111\rangle$)

n-qubit states live in a 2^n-dimensional space

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ... 32-dimensional space
($|00000\rangle$, $|00001\rangle$, ... $|11111\rangle$)

n-qubit states live in a 2^n-dimensional space

m-qubit states live in a 2^m-dimensional space

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ... 32-dimensional space
($|00000\rangle$, $|00001\rangle$, ... $|11111\rangle$)

n-qubit states live in a 2^n-dimensional space

m-qubit states live in a 2^m-dimensional space

$n + m$-qubit states live in a 2^{n+m}-dimensional space

Postulate II - composing systems
Intuition

We saw that the qubit is a ray/vector in a 2-dimensional space

A 2 qubit system should be a ray in a ... 4-dimensional space
($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$)

A 5 qubit system should be a ray in a ... 32-dimensional space
($|00000\rangle$, $|00001\rangle$, ... $|11111\rangle$)

n-qubit states live in a 2^n-dimensional space

m-qubit states live in a 2^m-dimensional space

$n + m$-qubit states live in a 2^{n+m}-dimensional space

If we have a 2^n dimensional vector and a 2^m dimensional vector
how do we get to the 2^{m+n} one?

Postulate II - composing systems

Postulate II - composing systems

Quantum states of a composite system live in a Hilbert space which is the tensor product of the Hilbert spaces of its components.

Postulate II

What is tensor product?

Postulate II

What is tensor product?

An example will help us understand...

Postulate II

Postulate II

Say our quantum computer has $N = 2$ qubits, so $R = [R_1 R_2]$

Postulate II

Say our quantum computer has $N = 2$ qubits, so $R = [R_1 R_2]$

So v_R is a 4-dimensional vector

Postulate II

Say our quantum computer has $N = 2$ qubits, so $R = [R_1 R_2]$

So v_R is a 4-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; v_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Postulate II

Say our quantum computer has $N = 2$ qubits, so $R = [R_1 R_2]$

So v_R is a 4-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ v_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$v_0 \leftrightarrow |00\rangle,\ v_1 \leftrightarrow |01\rangle,\ v_2 \leftrightarrow |10\rangle,\ v_3 \leftrightarrow |11\rangle$$

Postulate II

Say our quantum computer has $N = 2$ qubits, so $R = [R_1 R_2]$

So v_R is a 4-dimensional vector

$$v_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; v_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$v_0 \leftrightarrow |00\rangle, \; v_1 \leftrightarrow |01\rangle, \; v_2 \leftrightarrow |10\rangle, \; v_3 \leftrightarrow |11\rangle$$

Arbitrary vector

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$
$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

Postulate II

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Tensor product $\otimes$

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Tensor product $\otimes$

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\ c \\ a\ d \\ b\ c \\ b\ d \end{pmatrix}$$

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Tensor product $\otimes$

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\ c \\ a\ d \\ b\ c \\ b\ d \end{pmatrix}$$

$$(a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) =$$
$$ac\,|0\rangle \otimes |0\rangle + ad\,|0\rangle \otimes |1\rangle + bc\,|1\rangle \otimes |0\rangle + bd\,|1\rangle \otimes |1\rangle$$

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Tensor product $\otimes$

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\ c \\ a\ d \\ b\ c \\ b\ d \end{pmatrix}$$

$$(a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) =$$
$$ac\,|0\rangle \otimes |0\rangle + ad\,|0\rangle \otimes |1\rangle + bc\,|1\rangle \otimes |0\rangle + bd\,|1\rangle \otimes |1\rangle$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \iff |0\rangle \otimes |0\rangle = |00\rangle$$

Postulate II

But $|00\rangle$ is a composite system of two qubits $|0\rangle$

How to get from two $|0\rangle$'s to $|00\rangle$?

Tensor product $\otimes$

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\ c \\ a\ d \\ b\ c \\ b\ d \end{pmatrix}$$

$$(a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) =$$
$$ac\,|0\rangle \otimes |0\rangle + ad\,|0\rangle \otimes |1\rangle + bc\,|1\rangle \otimes |0\rangle + bd\,|1\rangle \otimes |1\rangle$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \iff |0\rangle \otimes |0\rangle = |00\rangle$$

$$|01\rangle = |0\rangle \otimes |1\rangle,\ |10\rangle = |1\rangle \otimes |0\rangle,\ |11\rangle = |1\rangle \otimes |1\rangle$$

Postulate II in reverse

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Say $|\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Say $|\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

$$|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$$
$$|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Say $|\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

$$|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$$
$$|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

$$\text{Say } |\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$$
$$|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

$$a_1 a_2 = 1/\sqrt{2} \quad a_1 b_2 = 0 \quad b_1 a_2 = 0 \quad b_1 b_2 = 1/\sqrt{2}$$

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Say $|\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

$$|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$$
$$|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

$$a_1 a_2 = 1/\sqrt{2} \quad a_1 b_2 = 0 \quad b_1 a_2 = 0 \quad b_1 b_2 = 1/\sqrt{2}$$

Not possible!

Postulate II in reverse

Take the 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In vector form: $v_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Which 2 states in tensor product yield this state?

None!

Say $|\psi_1\rangle \otimes |\psi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

$$|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$$
$$|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

$$a_1 a_2 = 1/\sqrt{2} \quad a_1 b_2 = 0 \quad b_1 a_2 = 0 \quad b_1 b_2 = 1/\sqrt{2}$$

Not possible!

These are called **entangled** states, rest are **separable** states

Entanglement

Entanglement

Do entangled states contradict postulate II?

Entanglement

Do entangled states contradict postulate II?

No!

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

The composite system has basis:
$\mathcal{B}_{12} = \{|b_1\rangle \otimes |b'_1\rangle, \ldots, |b_2\rangle \otimes |b'_1\rangle, \ldots |b_n\rangle \otimes |b'_m\rangle\}$

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

The composite system has basis:
$\mathcal{B}_{12} = \{|b_1\rangle \otimes |b'_1\rangle, \ldots, |b_2\rangle \otimes |b'_1\rangle, \ldots |b_n\rangle \otimes |b'_m\rangle\}$

This does not imply that general superpositions of $\mathcal{B}_{12}$ can be written in terms of a tensor product of superpositions of $\mathcal{B}_1$ and $\mathcal{B}_2$

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

The composite system has basis:
$\mathcal{B}_{12} = \{|b_1\rangle \otimes |b'_1\rangle, \ldots, |b_2\rangle \otimes |b'_1\rangle, \ldots |b_n\rangle \otimes |b'_m\rangle\}$

This does not imply that general superpositions of $\mathcal{B}_{12}$ can be written in terms of a tensor product of superpositions of $\mathcal{B}_1$ and $\mathcal{B}_2$

"*The whole is more than just the sum of its parts*"

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

The composite system has basis:
$\mathcal{B}_{12} = \{|b_1\rangle \otimes |b'_1\rangle, \ldots, |b_2\rangle \otimes |b'_1\rangle, \ldots |b_n\rangle \otimes |b'_m\rangle\}$

This does not imply that general superpositions of $\mathcal{B}_{12}$ can be written in terms of a tensor product of superpositions of $\mathcal{B}_1$ and $\mathcal{B}_2$

"*The whole is more than just the sum of its parts*"

Do entangled states contradict postulate I?

Entanglement

Do entangled states contradict postulate II?

No!

Postulate II essentially says that if you have 2 systems with bases:
$\mathcal{B}_1 = \{|b_1\rangle, \ldots |b_n\rangle\}$, $\mathcal{B}_2 = \{|b'_1\rangle, \ldots |b'_m\rangle\}$

The composite system has basis:
$\mathcal{B}_{12} = \{|b_1\rangle \otimes |b'_1\rangle, \ldots, |b_2\rangle \otimes |b'_1\rangle, \ldots |b_n\rangle \otimes |b'_m\rangle\}$

This does not imply that general superpositions of $\mathcal{B}_{12}$ can be written in terms of a tensor product of superpositions of $\mathcal{B}_1$ and $\mathcal{B}_2$

"*The whole is more than just the sum of its parts*"

Do entangled states contradict postulate I?

No! States are not isolated

Postulate III - dynamics
Intuition

Postulate III - dynamics
Intuition

How can we change the state of a system?

Postulate III - dynamics
Intuition

How can we change the state of a system?

As we've seen, either by applying a unitary matrix or measurement

Postulate III - dynamics
Intuition

How can we change the state of a system?

As we've seen, either by applying a unitary matrix or measurement

Focus on unitarity for now

Postulate III - dynamics
Intuition

How can we change the state of a system?

As we've seen, either by applying a unitary matrix or measurement

Focus on unitarity for now

Why unitary evolution?

Postulate III - dynamics
Intuition

How can we change the state of a system?

As we've seen, either by applying a unitary matrix or measurement

Focus on unitarity for now

Why unitary evolution?

Linear and it preserves the square norm

Postulate III - dynamics

Postulate III - dynamics

The evolution of an isolated (closed) quantum system is governed by unitary operators.

Postulate III

Postulate III

- An operator, U, is unitary iff $U^\dagger U = UU^\dagger = I$

Postulate III

- An operator, U, is unitary iff $U^\dagger U = UU^\dagger = I$
- $U^\dagger$ is the **adjoint** of U

Postulate III

- An operator, U, is unitary iff $U^\dagger U = UU^\dagger = I$
- $U^\dagger$ is the **adjoint** of U
- Where $U^\dagger$ is $\overline{U}^T$

Postulate III

- An operator, U, is unitary iff $U^\dagger U = UU^\dagger = I$
- $U^\dagger$ is the **adjoint** of U
- Where $U^\dagger$ is $\overline{U}^T$
- Never forget that these are **linear**!

Postulate III

- An operator, U, is unitary iff $U^\dagger U = UU^\dagger = I$
- $U^\dagger$ is the **adjoint** of U
- Where $U^\dagger$ is $\overline{U}^T$
- Never forget that these are **linear**!
- We'll see next week, postulate III is equivalent to **Schrödinger's equation**

$$\left(-\frac{\hbar^2}{2m}\nabla^2 + V\right)\psi = i\hbar\frac{\partial\psi}{\partial t}$$

Postulate III

Postulate III

- Note that $U^\dagger$ is also unitary!

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible
- If $U|\psi\rangle = |\phi\rangle$, then $U^\dagger|\phi\rangle = |\psi\rangle$

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible
- If $U|\psi\rangle = |\phi\rangle$, then $U^\dagger|\phi\rangle = |\psi\rangle$
- As long as we don't measure, everything we do is reversible

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible
- If $U|\psi\rangle = |\phi\rangle$, then $U^\dagger|\phi\rangle = |\psi\rangle$
- As long as we don't measure, everything we do is reversible
- Interesting side note: $n \times n$ unitaries form a group called $U(n)$

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible
- If $U|\psi\rangle = |\phi\rangle$, then $U^\dagger|\phi\rangle = |\psi\rangle$
- As long as we don't measure, everything we do is reversible
- Interesting side note: $n \times n$ unitaries form a group called $U(n)$
- If we also impose $det(U) = 1$, we get the group $SU(n)$

Postulate III

- Note that $U^\dagger$ is also unitary!
- Operations are invertible
- If $U|\psi\rangle = |\phi\rangle$, then $U^\dagger|\phi\rangle = |\psi\rangle$
- As long as we don't measure, everything we do is reversible
- Interesting side note: $n \times n$ unitaries form a group called $U(n)$
- If we also impose $det(U) = 1$, we get the group $SU(n)$
- These groups have tremendous importance in physics as *symmetry* groups

Postulate III
Single qubit examples

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

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

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

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

Pauli matrices

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

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

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

Pauli matrices

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

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

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

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

Pauli matrices

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

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

$$Y|0\rangle = i|1\rangle,\; Y|1\rangle = -i|0\rangle$$

Postulate III
Single qubit examples

$$\text{Hadamard } H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

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

Pauli matrices

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

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

$$Y|0\rangle = i|1\rangle,\; Y|1\rangle = -i|0\rangle$$

$$Z|0\rangle = |0\rangle,\; Z|1\rangle = -|1\rangle$$

Postulate III
Multi-qubit examples

Postulate III
Multi-qubit examples

$$\text{Controlled-Not } CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Postulate III
Multi-qubit examples

$$\text{Controlled-Not } CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT\,|00\rangle = |00\rangle,\ CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle,\ CNOT\,|11\rangle = |10\rangle$$

Postulate III
Multi-qubit examples

$$\text{Controlled-Not } CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT\,|00\rangle = |00\rangle,\ CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle,\ CNOT\,|11\rangle = |10\rangle$$

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

Postulate III
Multi-qubit examples

$$\text{Controlled-Not } CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT\,|00\rangle = |00\rangle,\ CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle,\ CNOT\,|11\rangle = |10\rangle$$

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

$$CZ\,|00\rangle = |00\rangle,\ CZ\,|01\rangle = |01\rangle$$
$$CZ\,|10\rangle = |10\rangle,\ CZ\,|11\rangle = -\,|11\rangle$$

Postulate III
Multi-qubit examples

What if we have two qubits and flip (Pauli X) both of them?
What's the corresponding unitary?

Postulate III
Multi-qubit examples

What if we have two qubits and flip (Pauli X) both of them?
What's the corresponding unitary?

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

Postulate III
Multi-qubit examples

What if we have two qubits and flip (Pauli X) both of them?
What's the corresponding unitary?

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

In general

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$

Postulate III
Acting on general states

Postulate III
Acting on general states

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

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \frac{a+b}{\sqrt{2}}\,|0\rangle + \frac{a-b}{\sqrt{2}}\,|1\rangle$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \tfrac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \tfrac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \tfrac{a+b}{\sqrt{2}}\,|0\rangle + \tfrac{a-b}{\sqrt{2}}\,|1\rangle$$

$$X\,|\psi\rangle = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \tfrac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \tfrac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \tfrac{a+b}{\sqrt{2}}\,|0\rangle + \tfrac{a-b}{\sqrt{2}}\,|1\rangle$$

$$X\,|\psi\rangle = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

$$Z\,|\psi\rangle = aZ\,|0\rangle + bZ\,|1\rangle = a\,|0\rangle - b\,|1\rangle$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \tfrac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \tfrac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \tfrac{a+b}{\sqrt{2}}\,|0\rangle + \tfrac{a-b}{\sqrt{2}}\,|1\rangle$$

$$X\,|\psi\rangle = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

$$Z\,|\psi\rangle = aZ\,|0\rangle + bZ\,|1\rangle = a\,|0\rangle - b\,|1\rangle$$

$$|\chi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \frac{a+b}{\sqrt{2}}\,|0\rangle + \frac{a-b}{\sqrt{2}}\,|1\rangle$$

$$X\,|\psi\rangle = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

$$Z\,|\psi\rangle = aZ\,|0\rangle + bZ\,|1\rangle = a\,|0\rangle - b\,|1\rangle$$

$$|\chi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

$$CNOT\,|\chi\rangle =$$
$$aCNOT\,|00\rangle + bCNOT\,|01\rangle + cCNOT\,|10\rangle + dCNOT\,|11\rangle$$

Postulate III
Acting on general states

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

$$H\,|\psi\rangle = aH\,|0\rangle + bH\,|1\rangle = \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H\,|\psi\rangle = \frac{a+b}{\sqrt{2}}\,|0\rangle + \frac{a-b}{\sqrt{2}}\,|1\rangle$$

$$X\,|\psi\rangle = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

$$Z\,|\psi\rangle = aZ\,|0\rangle + bZ\,|1\rangle = a\,|0\rangle - b\,|1\rangle$$

$$|\chi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

$$CNOT\,|\chi\rangle =$$
$$aCNOT\,|00\rangle + bCNOT\,|01\rangle + cCNOT\,|10\rangle + dCNOT\,|11\rangle$$

$$CNOT\,|\chi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$$

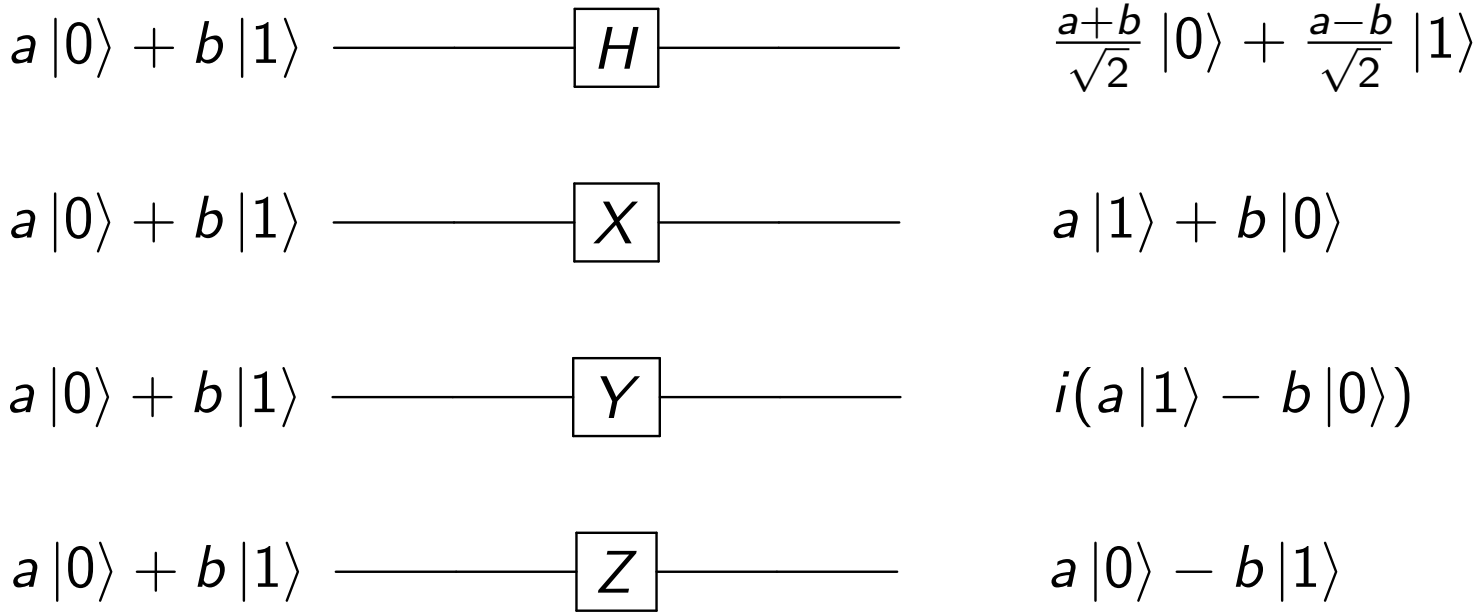
The circuit picture

The circuit picture

Everything we just mentioned can be represented as circuits

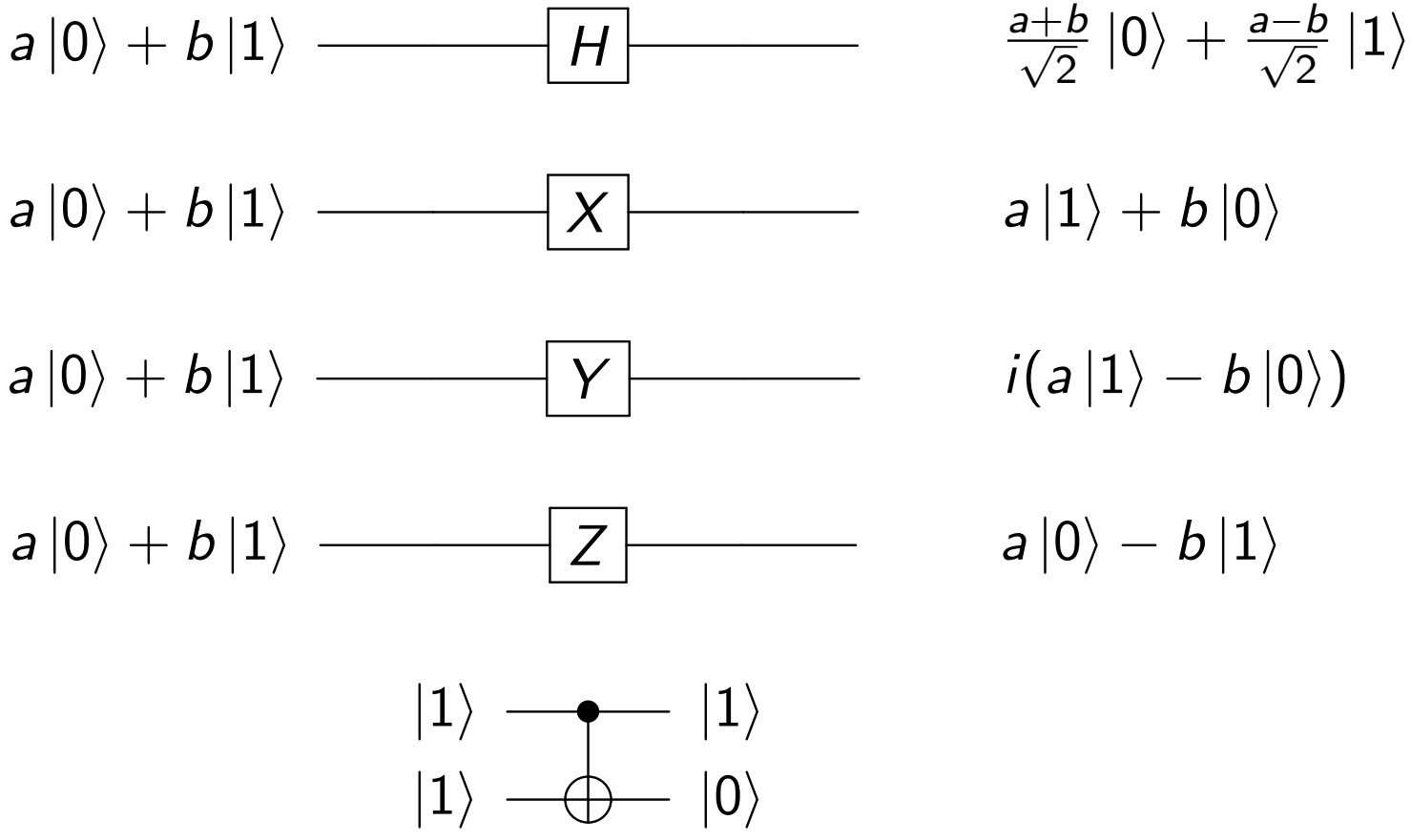
The circuit picture

Everything we just mentioned can be represented as circuits



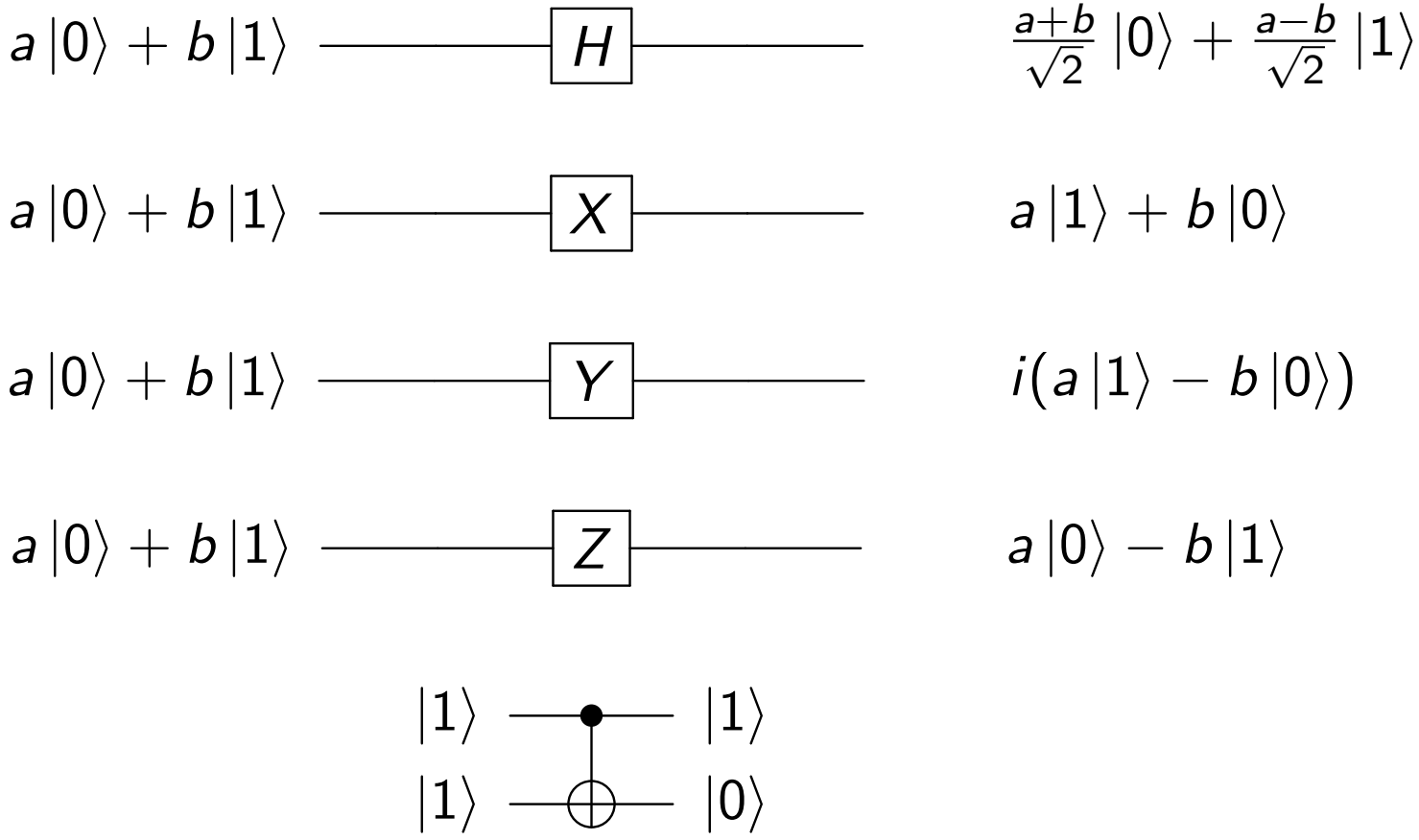
The circuit picture

Everything we just mentioned can be represented as circuits



The circuit picture

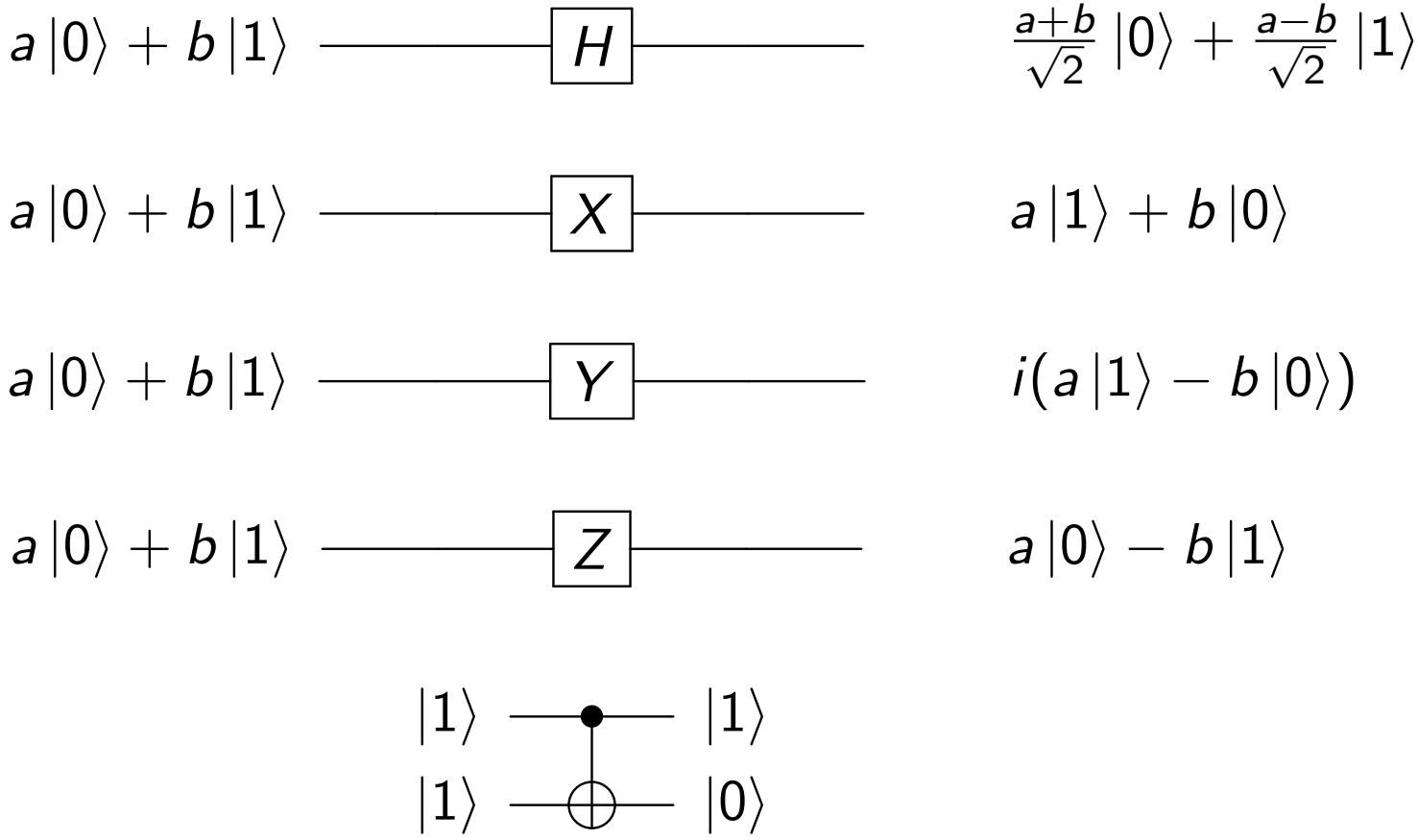
Everything we just mentioned can be represented as circuits



Note that all these gates/operators are their own inverses

The circuit picture

Everything we just mentioned can be represented as circuits



Note that all these gates/operators are their own inverses

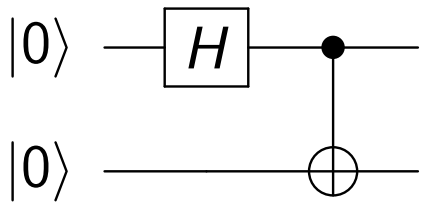
So the pictures are valid in both directions!

The circuit picture

What is the output for the following circuit?

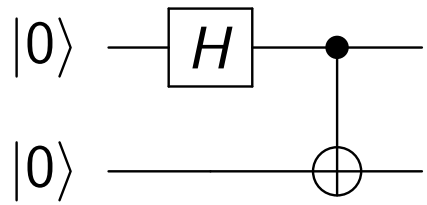
The circuit picture

What is the output for the following circuit?



The circuit picture

What is the output for the following circuit?

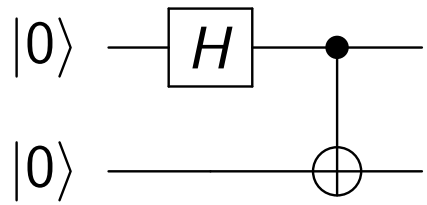


After first layer, we have:

$(H \otimes I)\,|00\rangle =$

The circuit picture

What is the output for the following circuit?

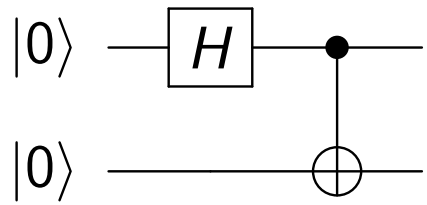


After first layer, we have:

$$(H \otimes I)\,|00\rangle = (H \otimes I)(|0\rangle \otimes |0\rangle) =$$

The circuit picture

What is the output for the following circuit?

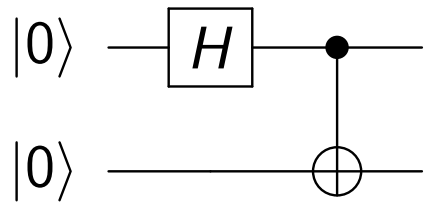


After first layer, we have:

$$(H \otimes I)\,|00\rangle = (H \otimes I)(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

The circuit picture

What is the output for the following circuit?



After first layer, we have:

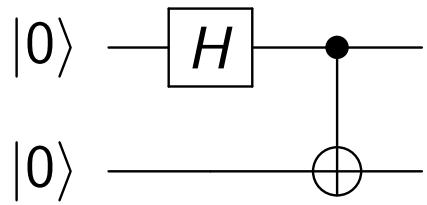
$$(H \otimes I)\,|00\rangle = (H \otimes I)(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

After second layer, we have:

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

The circuit picture

What is the output for the following circuit?



After first layer, we have:

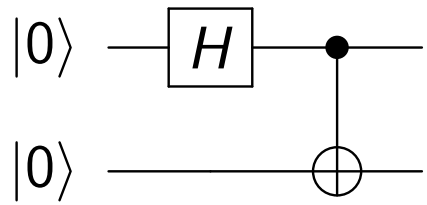
$$(H \otimes I)\,|00\rangle = (H \otimes I)(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

After second layer, we have:

$$CNOT\ \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(CNOT\,|00\rangle + CNOT\,|10\rangle)$$

The circuit picture

What is the output for the following circuit?



$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

After first layer, we have:

$$(H \otimes I)\,|00\rangle = (H \otimes I)(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

After second layer, we have:

$$CNOT\ \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(CNOT\,|00\rangle + CNOT\,|10\rangle)$$

So we end up with:

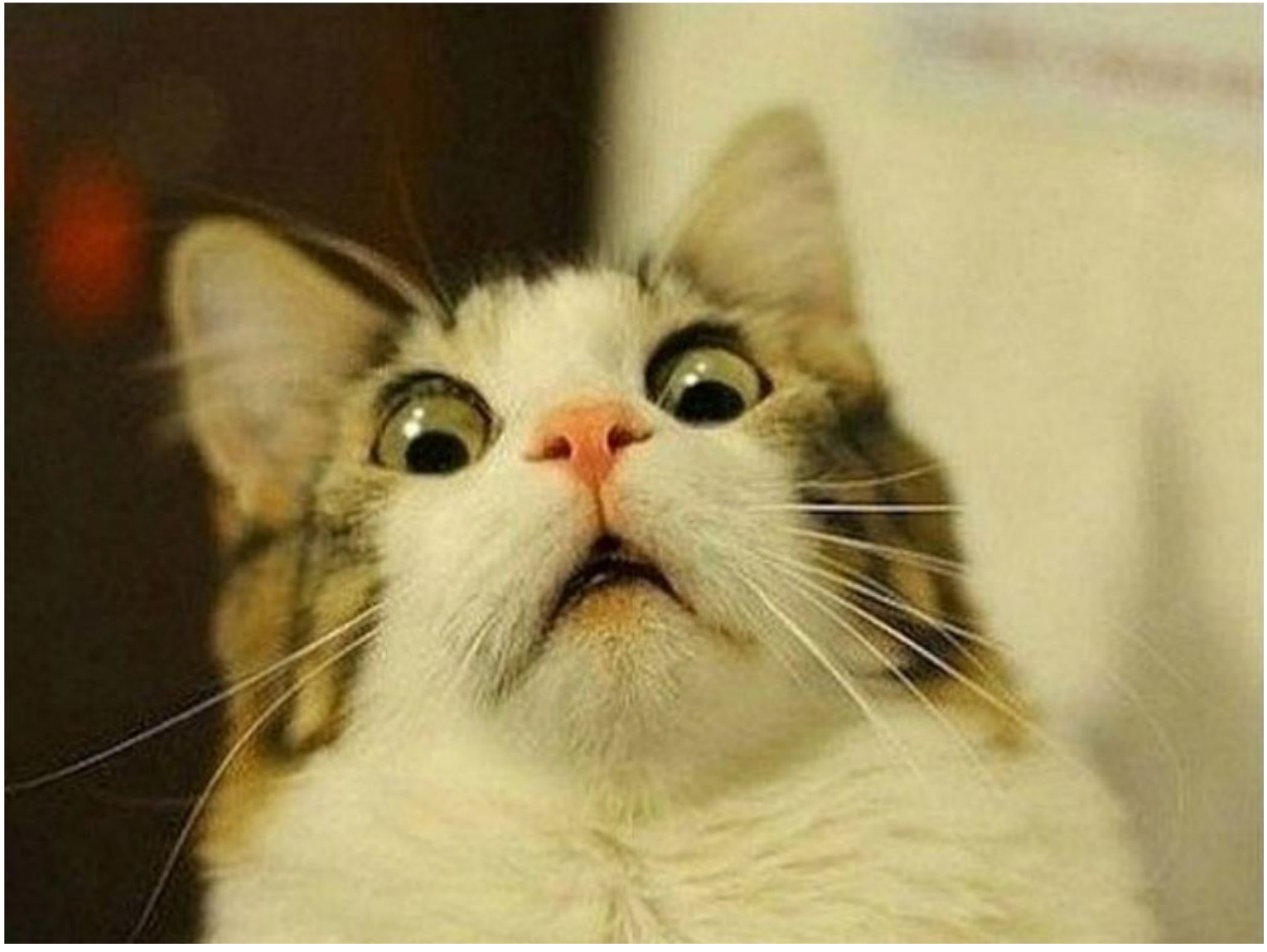
$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

Postulate IV - observation

Brace yourselves...

Postulate IV - observation

The properties that can be observed about a quantum system are called observables. They correspond to Hermitian operators. The observed values are the eigenvalues of these operators, and the system "collapses" to the corresponding eigenstate. The probabilities of observation and collapse are given by Born's rule.



To be explained in part 2! :)

Useful resources and references

- **A nice quantum computing lecture** - https://qcintro.wordpress.com/lectures/
- **A nice introduction to quantum computing** - http://arxiv.org/pdf/0708.0261v1.pdf
- **Quantum computing for non-physicists** - http://arxiv.org/pdf/quant-ph/9809016v2.pdf
- **A more mathematical lecture** - http://www.theory.caltech.edu/~preskill/ph219/
- **Quantum theory from five reasonable axioms** - http://arxiv.org/pdf/quant-ph/0101012v4.pdf
- **Density matrix formalism** - http://www.cithep.caltech.edu/~fcp/physics/quantumMechanics/densityMatrix/densityMatrix.pdf

Useful resources and references

- **Postulates of QM** - any quantum mechanics textbook. Recommended: Introduction to Quantum Mechanics, http://www.amazon.com/Introduction-Quantum-Mechanics-2nd-Edition/dp/0131118927
- **Postulates applied to computing and anything about quantum information** - Quantum Computation and Quantum Information, http://www.amazon.com/Quantum-Computation-Information-Anniversary-Edition/dp/1107002176
- Image on slide 4 (comparison) - http://download2.cerimes.fr/canalu/documents/fuscia/quantum.turing.test_13249/kashefi.pdf
- Image on slide 13 (SMBC comic) - http://www.smbc-comics.com/comic/2011-04-21
- Image on slide 34 (cat reaction) - http://dailynewsdig.com/wp-content/uploads/2013/06/20-Funny-Shocked-Cat-Memes-3.jpg