Mecânica quântica para computação

Bento Montenegro

Qiskit | Fall Fest 2023

Introdução

A computação quântica é uma das grandes tecnologias em emergência da nossa época. Mas por quê? E como funciona exatamente?

Introdução

A computação quântica é uma das grandes tecnologias em emergência da nossa época. Mas por quê? E como funciona exatamente?

- Existem problemas que são extremamente difíceis (ou mesmo impossíveis!) de se resolver em um computador usual.

Introdução

A computação quântica é uma das grandes tecnologias em emergência da nossa época. Mas por quê? E como funciona exatamente?

- Existem problemas que são extremamente difíceis (ou mesmo impossíveis!) de se resolver em um computador usual.
  - O exemplo mais comum é o **algoritmo de Shor** para **fatoração em números primos**.

Introdução

A computação quântica é uma das grandes tecnologias em emergência da nossa época. Mas por quê? E como funciona exatamente?

- Existem problemas que são extremamente difíceis (ou mesmo impossíveis!) de se resolver em um computador usual.
    - O exemplo mais comum é o **algoritmo de Shor** para **fatoração em números primos**.

- Algoritmos de busca lineares também não são tão eficientes quanto sua contraparte quântica (**algoritmo de Grover**).

Introdução

A computação quântica é uma das grandes tecnologias em emergência da nossa época. Mas por quê? E como funciona exatamente?

- Computadores quânticos também auxiliarão de forma extremamente eficiente:
  - **Simulações em química** envolvendo dinâmica molecular
  - **Simulações em finanças** e prospectos econômicos
  - **Machine learning** e **desenvolvimento de IA's** mais potentes

Índice

Parte I

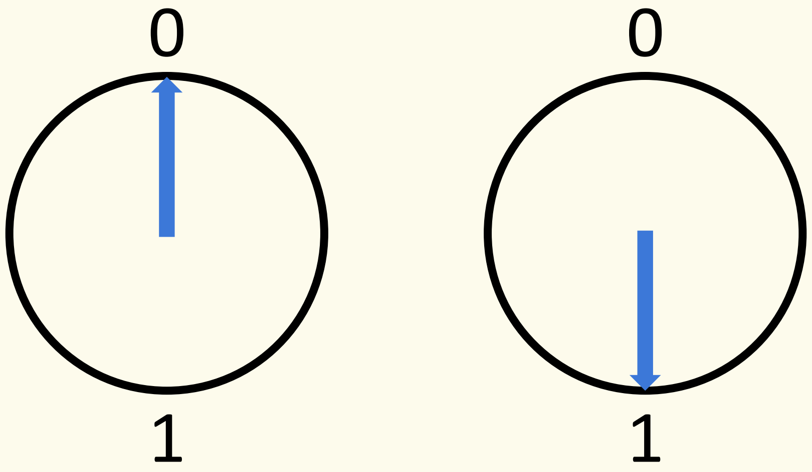
- Bits e qubits
- MQ para computação
  - Vetores de estado
  - Superposição
  - Medições

Parte II

- Esfera de Bloch
- Múltiplos qubits e emaranhamento

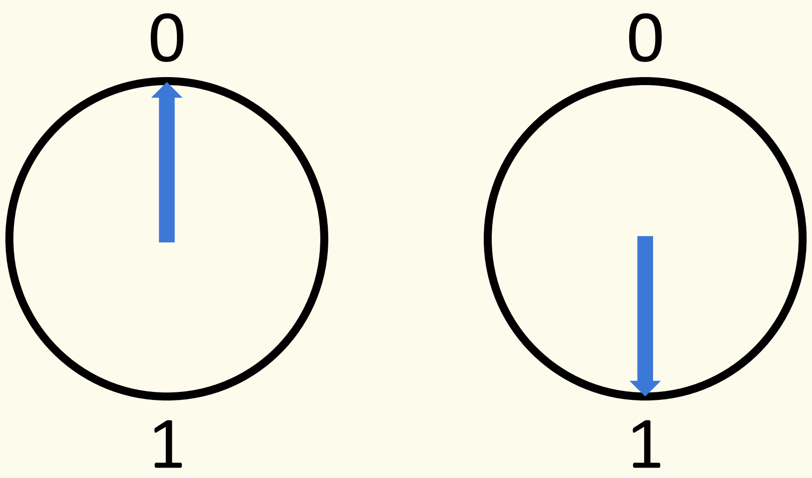
Bits e qubits

- Bit clássico (= bit): 0, 1

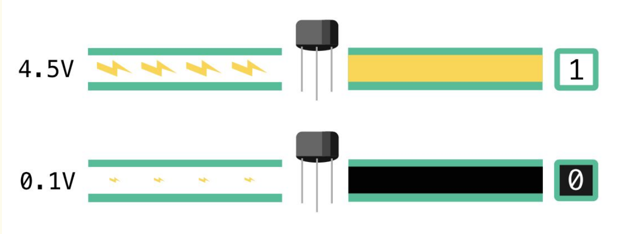


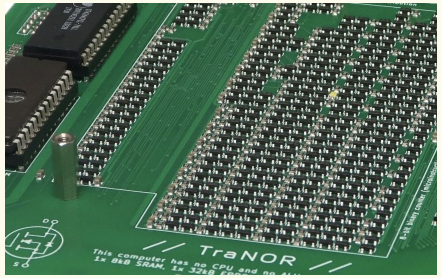
Bits e qubits

- Bit clássico (= bit): 0, 1



Fisicamente, bits são usualmente implementados como transistors



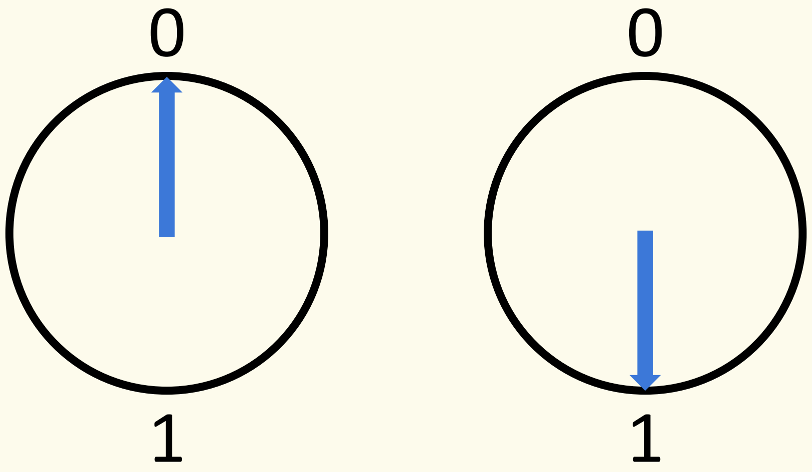


High-tech CPU

~ 10^9 transistors

Bits e qubits

- Bit clássico (= bit): 0, 1



Números são representados como strings de 0's e 1's

$2^0 = 1$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$

$$150 = 1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$

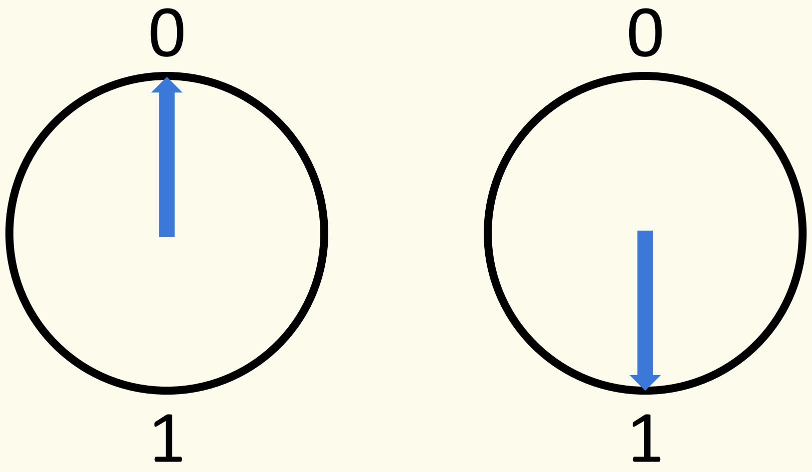
$$= 10010110$$

$$35 = 0 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

$$= 00100011$$

Bits e qubits

- Bit clássico (= bit): 0, 1



Computações são feitas de maneira similar ao ensino fundamental:

0 + 0 = 0

0 + 1 = 1

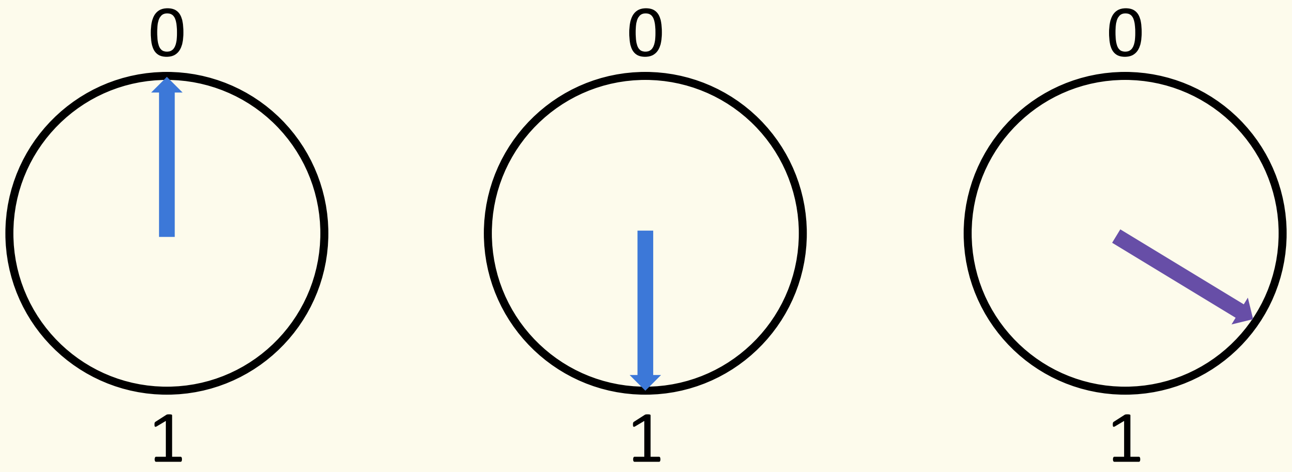
1 + 1 = 10

→ 150 + 35 =

$$
\begin{array}{r}
10010110 \\
+\ 00100011 \\
\hline
10111001
\end{array}
= 185
$$

Bits e qubits

- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1

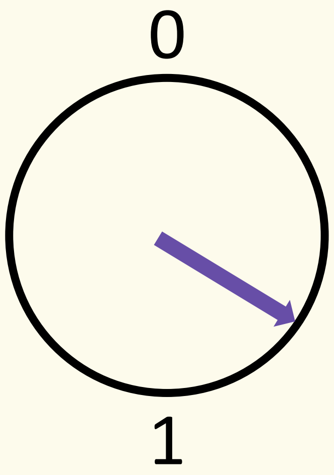


= tantos porcento em 0 +

tantos porcento em 1

Bits e qubits

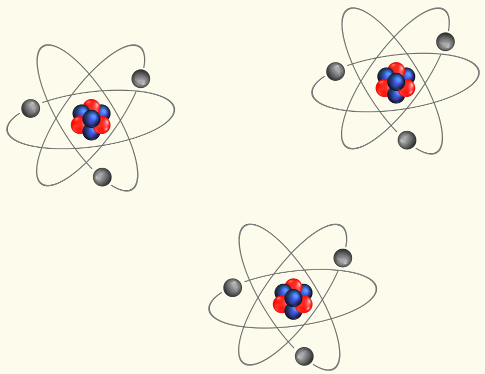
- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1



tantos porcento em 0

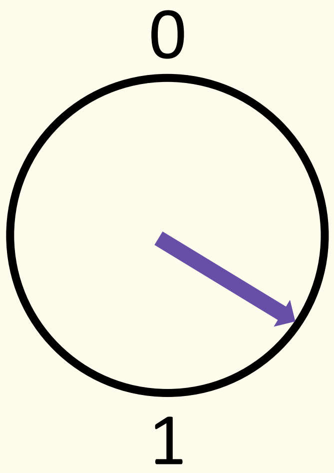
tantos porcento em 1

- Fisicamente, qubits são **átomos**



Bits e qubits

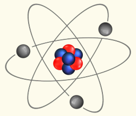
- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1

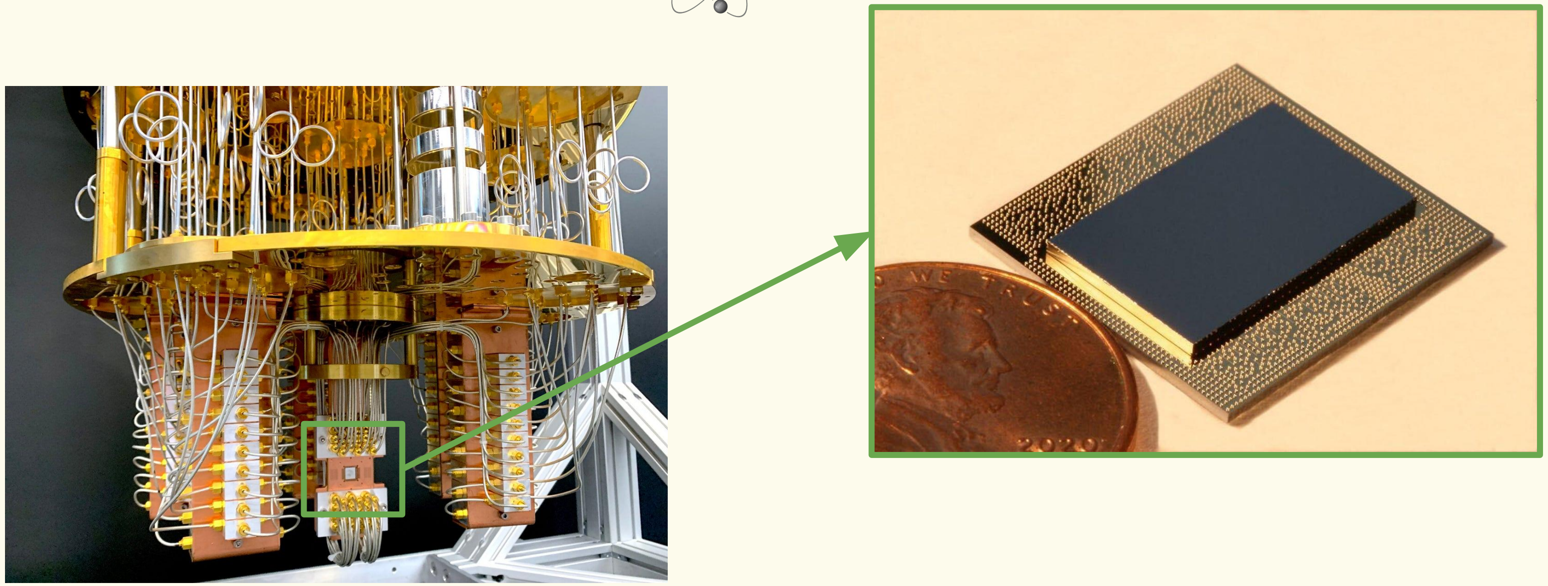


tantos porcento em 0

tantos porcento em 1

- Fisicamente, qubits são **átomos**

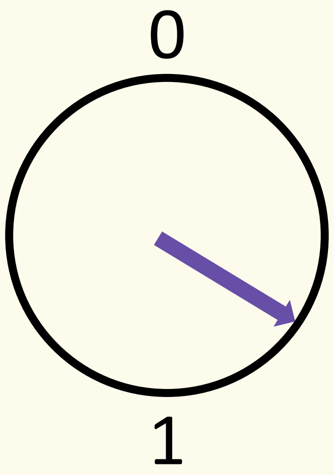




Computador quântico

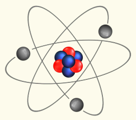
Bits e qubits

- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1



tantos porcento em 0

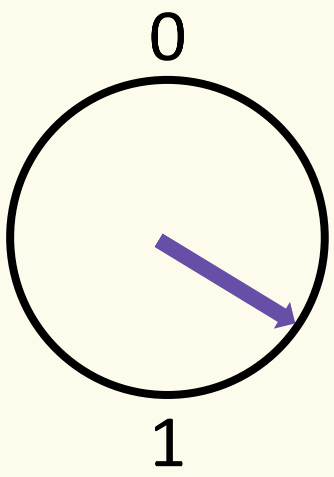
tantos porcento em 1

- Fisicamente, qubits são **átomos** 

- A teoria física capaz de descrever o comportamento dos átomos é a **mecânica quântica** (MQ)

Bits e qubits

- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1



tantos porcento em 0

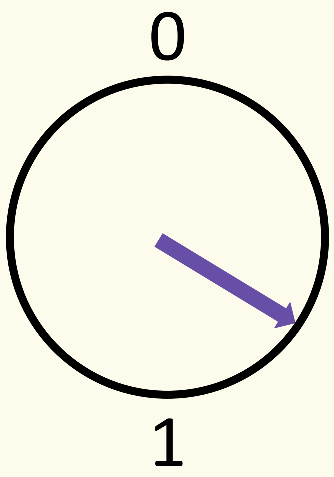
tantos porcento em 1

- De acordo com a MQ, os átomos obedecem às seguintes propriedades
  - Interferência
  - Superposição
  - Emaranhamento

- Alem disso, **coisas malucas acontecem quando "observamos" um átomo!**

Bits e qubits

- Bit quântico (= qubit): 0, 1, **superposição** de 0 e 1



tantos porcento em 0

tantos porcento em 1

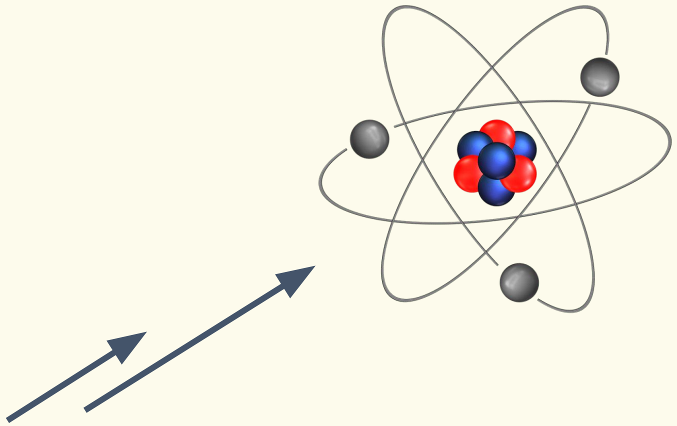
- De acordo com a MQ, os átomos obedecem às seguintes propriedades
  - Interferência
  - Superposição
  - Emaranhamento

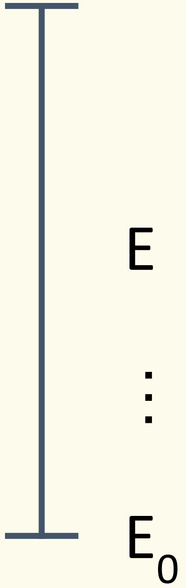
- Alem disso, **coisas malucas acontecem quando "observamos" um átomo!**

Computação quântica: explorar esses fatos para fazer computação

Superposição

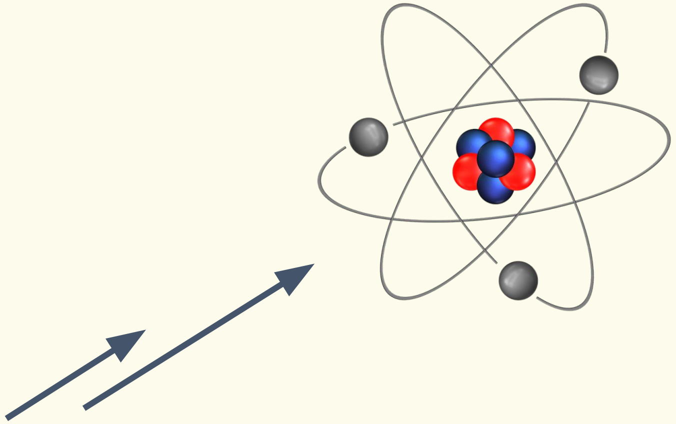
A MQ diz que quando medimos a energia de um átomo livre, podemos encontrar qualquer valor em um continuum

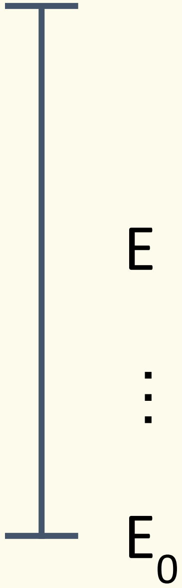




Superposição

A MQ diz que quando medimos a energia de um átomo livre, podemos encontrar qualquer valor em um continuum



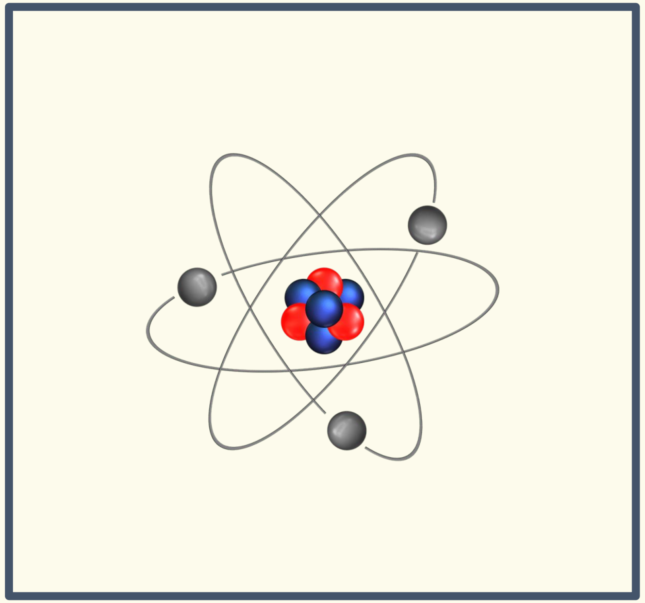


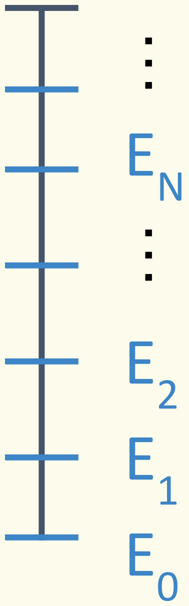
Até aqui nada de novo!

Coisas do dia-a-dia também se comportam assim

Superposição

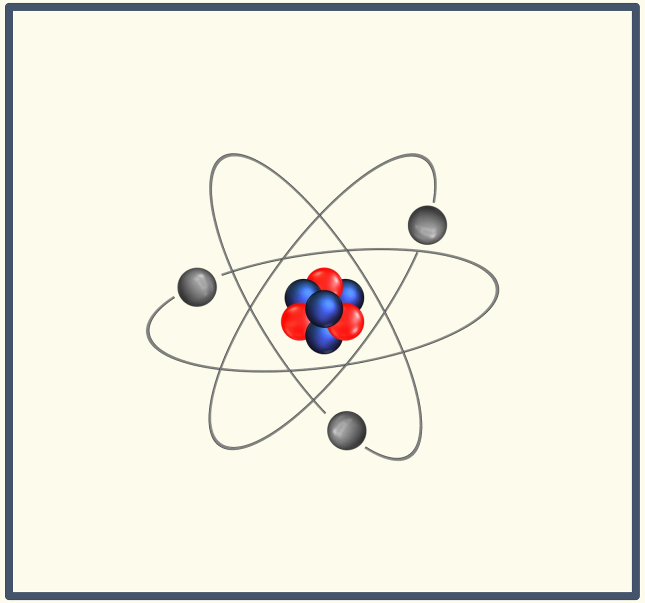
Entretanto, quando medimos a energia de um átomo **confinado**, apenas certos valores **discretos** são observados

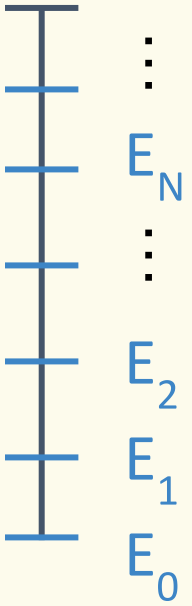




Superposição

Entretanto, quando medimos a energia de um átomo **confinado**, apenas certos valores **discretos** são observados

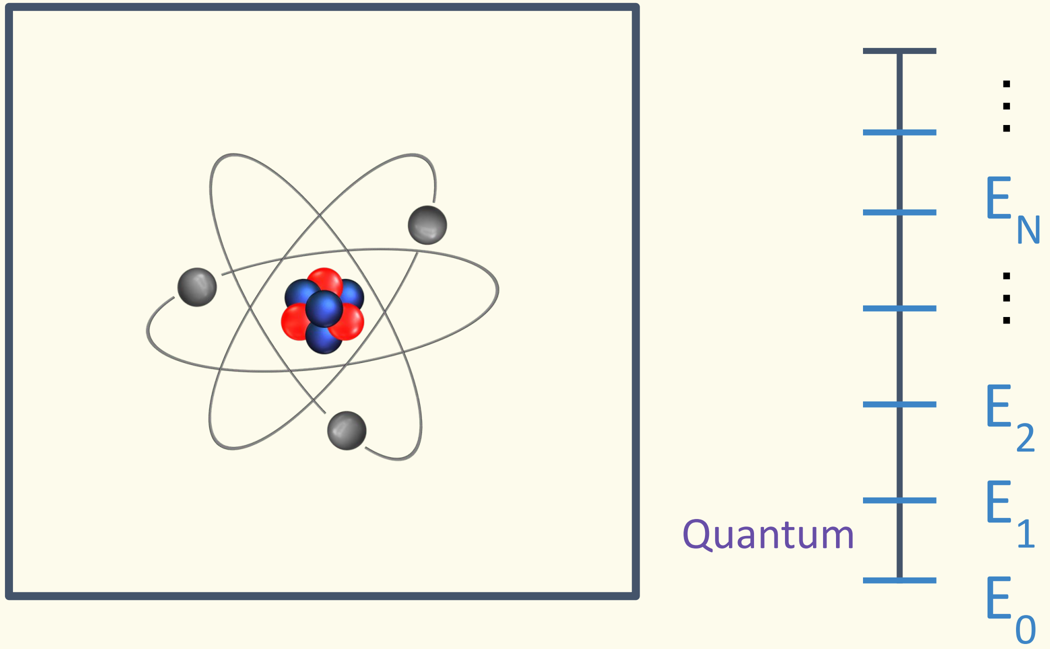




Fisicamente isso é uma consequência da dualidade **onda-partícula**

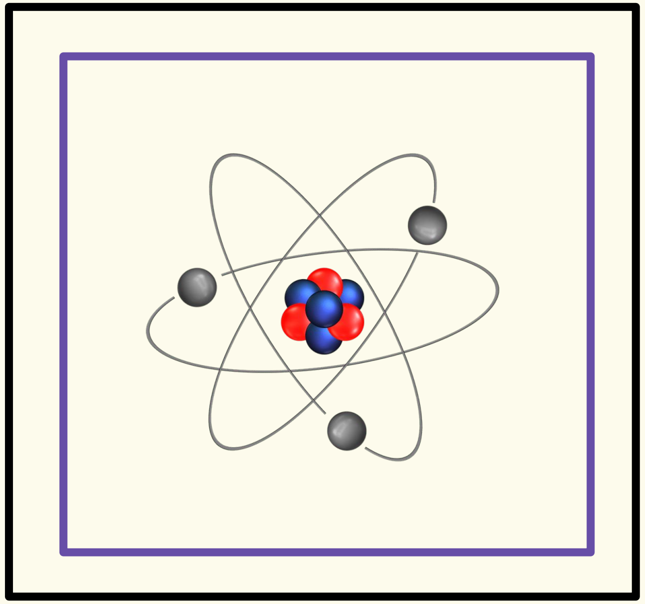
Superposição

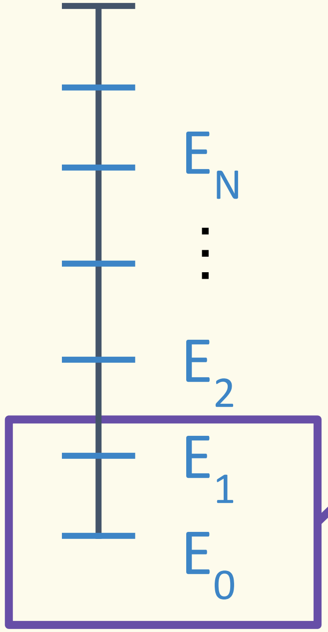
Por isso, dizemos que a energia do átomo é **quantizada**



Superposição

Mais ainda: experimentalmente, é possível confinar um átomo de tal maneira que só seja possível medir **dois valores** de energia





Notação:

Estado de energia E_0 = $|0\rangle$

Estado de energia E_1 = $|1\rangle$

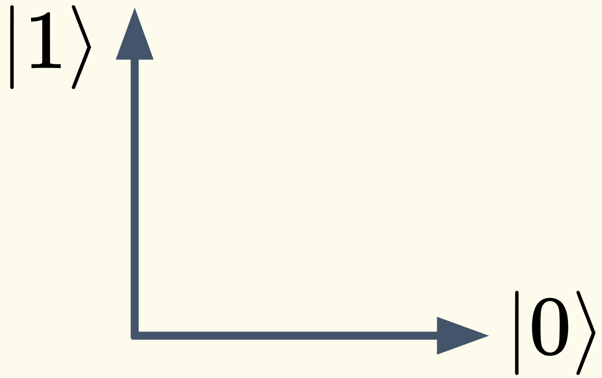
Qubit? \o/

Superposição

- Isto é, quando fazemos um experimento:
  - Se o resultado for E_1, descobrimos que o estado do átomo é $|0\rangle$
  - Se o resultado for E_2, descobrimos que o estado do átomo é $|1\rangle$

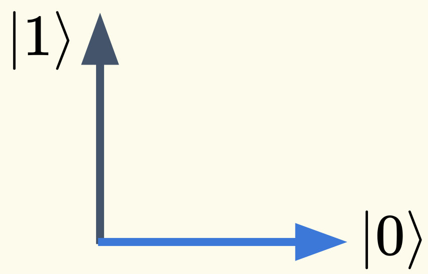
Superposição

- Isto é, quando fazemos um experimento:
    - Se o resultado for E_1, descobrimos que o estado do átomo é $|0\rangle$
    - Se o resultado for E_2, descobrimos que o estado do átomo é $|1\rangle$
- É conveniente organizar estes dois estados como dois **vetores ortogonais**

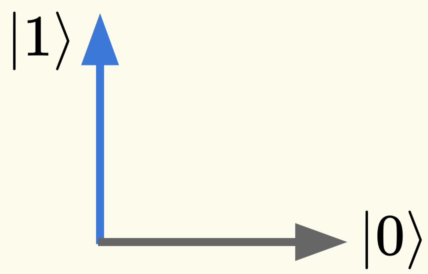


Superposição

Assim, quando observamos o átomo, ou ele colapsa no **estado zero**



ou ele colapsa no **estado um**



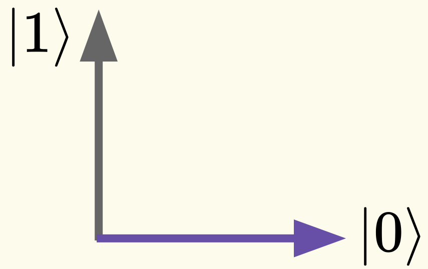
Superposição

Princípio da superposição: **antes de ser observado**, o átomo pode estar em qualquer combinação linear de seu conjunto de estados acessíveis

Superposição

Princípio da superposição: antes de ser observado, o átomo pode estar em qualquer combinação linear de seu conjunto de estados acessíveis

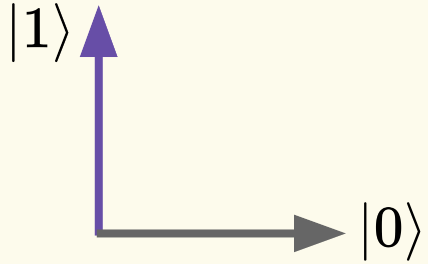
- Por exemplo, antes de ser observado, o átomo de dois níveis pode estar no estado
  - **Zero**
  - Um
  - Zero e um ao mesmo tempo



Superposição

Princípio da superposição: antes de ser observado, o átomo pode estar em qualquer combinação linear de seu conjunto de estados acessíveis

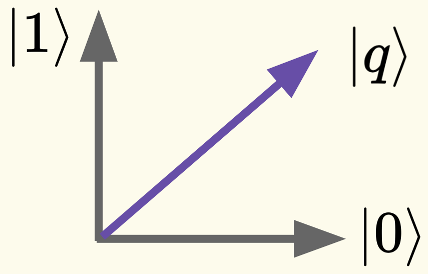
- Por exemplo, antes de ser observado, o átomo de dois níveis pode estar no estado
  - Zero
  - **Um**
  - Zero e um ao mesmo tempo



Superposição

Princípio da superposição: antes de ser observado, o átomo pode estar em qualquer combinação linear de seu conjunto de estados acessíveis

- Por exemplo, antes de ser observado, o átomo de dois níveis pode estar no estado
  - Zero
  - Um
  - **Zero e um** ao mesmo tempo!



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

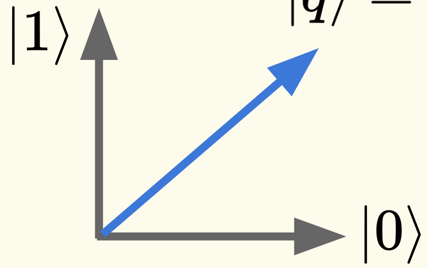
Superposição

- Mas sabemos que apenas um valor de energia é medido

- O que acontece então?

Antes de medir:

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



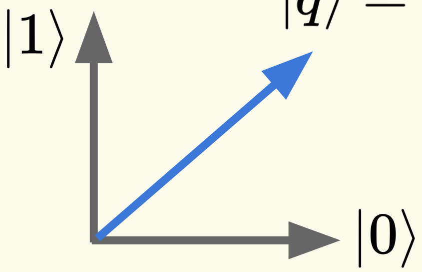
Superposição

- Mas sabemos que apenas um valor de energia é medido

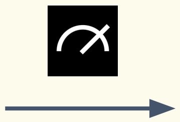
- O que acontece então?

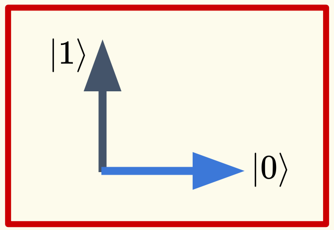
Antes de medir:

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

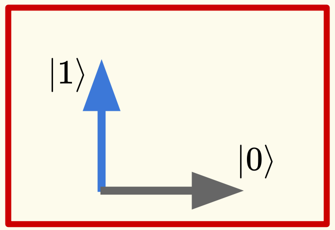


Medição





ou



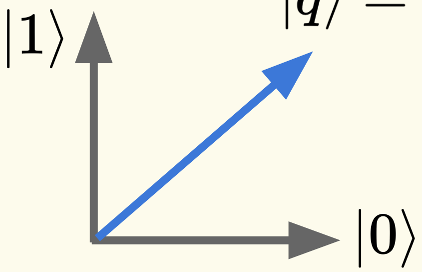
Superposição

- Mas sabemos que apenas um valor de energia é medido

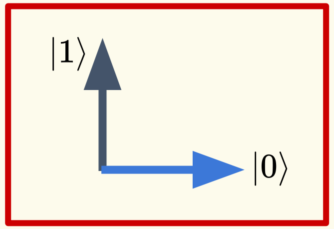
- O que acontece então?

Antes de medir:

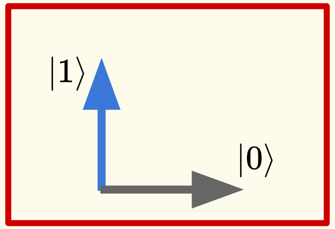
$$|q\rangle = a|0\rangle + b|1\rangle$$



Medição



ou



A medição **destrói** a superposição!

Medições

- Suponha agora que um átomo de vários níveis está no seguinte estado superposto

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \ldots$$

Medições

- Suponha agora que um átomo de vários níveis está no seguinte estado superposto

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \ldots$$

- Sabemos que **uma medição destrói a superposição**
  - Mas destrói **como** exatamente? 🤔

Medições

- Suponha agora que um átomo de vários níveis está no seguinte estado superposto

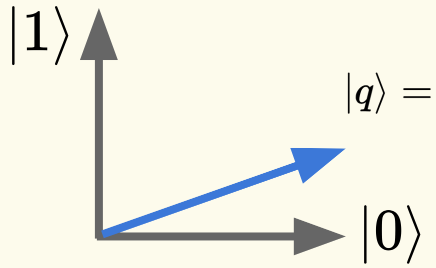
$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \dots$$

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

Antes de medir:

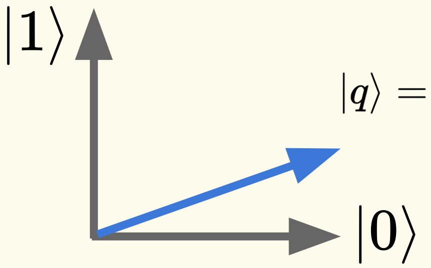


$$|q\rangle = \sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle$$

Medições

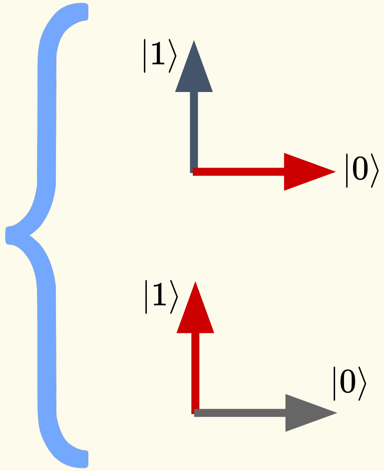
Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

Antes de medir:



$$|q\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

Medição



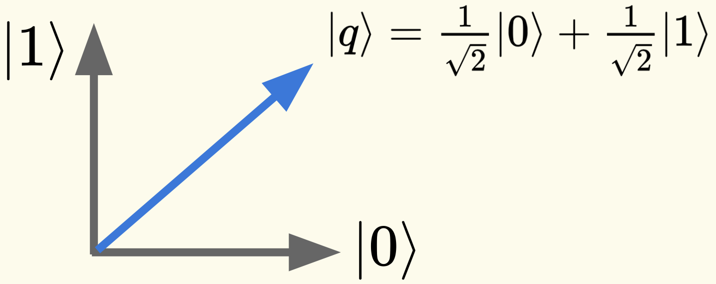
Com probabilidade $\left|\sqrt{\frac{2}{3}}\right|^2 = \frac{2}{3}$

Com probabilidade $\left|\frac{1}{\sqrt{3}}\right|^2 = \frac{1}{3}$

Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

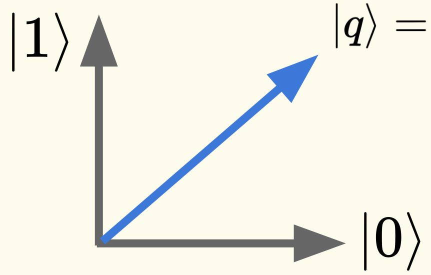
Antes de medir:



Medições

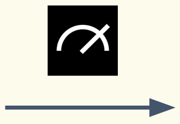
Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

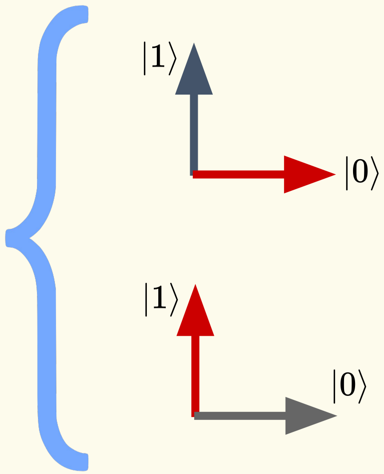
Antes de medir:



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

Medição





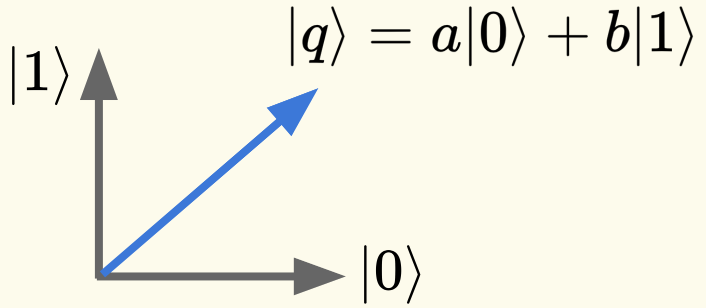
Com probabilidade $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

Com probabilidade $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

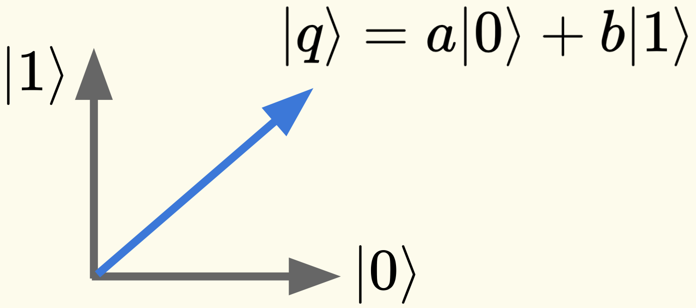
Antes de medir:

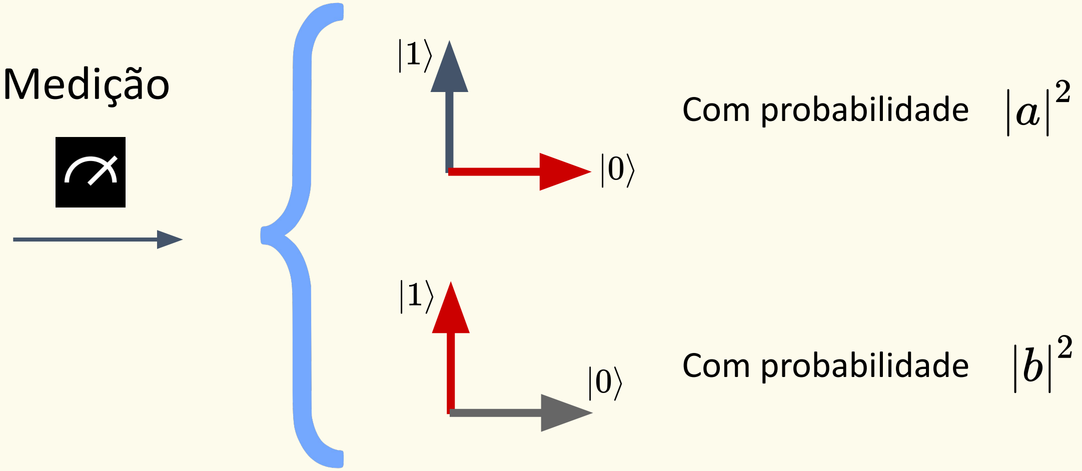


Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

Antes de medir:



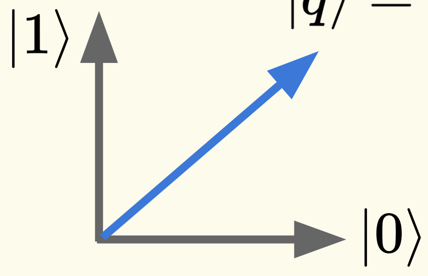


Medições

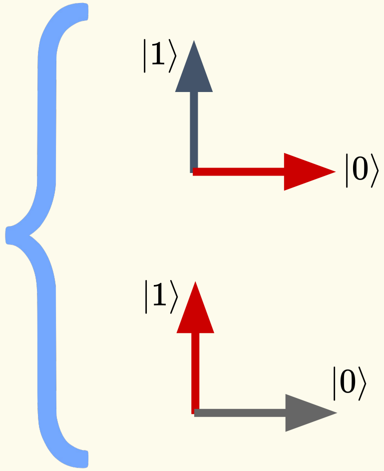
Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

Antes de medir:

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



Medição



Com probabilidade $|a|^2$

Com probabilidade $|b|^2$

É por isso que dizemos que a M é **probabilística!**

Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

- **Importante:** como "medir o estado i" é um evento **mutuamente excludente** com "medir o estado j" (i ≠ j), e a soma de todas as probabilidades deve ser 1, temos a seguinte condição:

$$|a_1|^2 + |a_2|^2 + \ldots + |a_N|^2 = 1$$

Medições

Regra de Born: a medição colapsa o átomo no estado $|i\rangle$ com probabilidade $|a_i|^2$

- **Importante:** como "medir o estado i" é um evento **mutuamente excludente** com "medir o estado j" (i ≠ j), e a soma de todas as probabilidades deve ser 1, temos a seguinte condição:

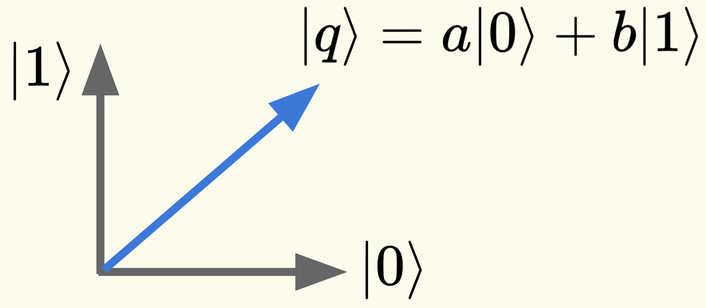
$$|a_1|^2 + |a_2|^2 + \ldots + |a_N|^2 = 1$$

Vetores de estado devem ser **normalizados**!

Regras básicas da MQ

Resumo da ópera

1. Átomos podem estar em uma **superposição** de estados

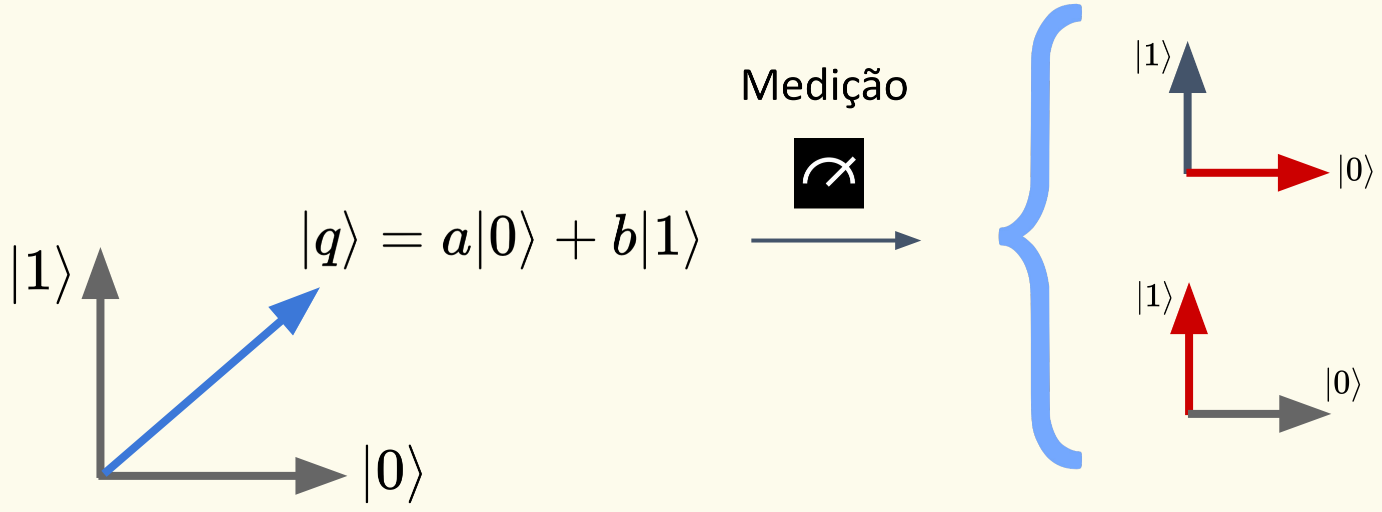


Regras básicas da MQ

Resumo da ópera

1. Átomos podem estar em uma **superposição** de estados

2. Medições destroem essa superposição segundo a **regra de Born**



Com probabilidade $|a|^2$

Com probabilidade $|b|^2$

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

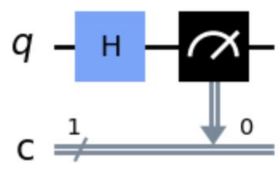
Qiskit | Fall Fest 2023

Circuitos de 1 qubit (prévia)

Logo mais aprenderemos a simular qubits e medições usando Qiskit!

```
In [11]: from qiskit import QuantumCircuit

         qc = QuantumCircuit(1, 1) # Criando um circuito de 1 qubit e 1 bit
         qc.h(0) # Pondo o qubit em uma superposição

         qc.measure(0, 0) # Medindo o estado do qubit e armazenando no bit

         qc.draw('mpl')
```

Out[11]:



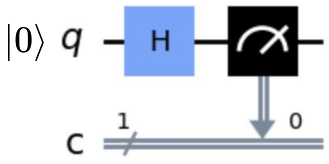
Circuitos de 1 qubit (prévia)

Logo mais aprenderemos a simular qubits e medições usando Qiskit!

In [11]:
```python
from qiskit import QuantumCircuit

qc = QuantumCircuit(1, 1) # Criando um circuito de 1 qubit e 1 bit
qc.h(0) # Pondo o qubit em uma superposição

qc.measure(0, 0) # Medindo o estado do qubit e armazenando no bit

qc.draw('mpl')
```

Out[11]:

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

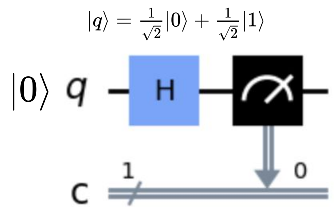


Circuitos de 1 qubit (prévia)

Logo mais aprenderemos a simular qubits e medições usando Qiskit!

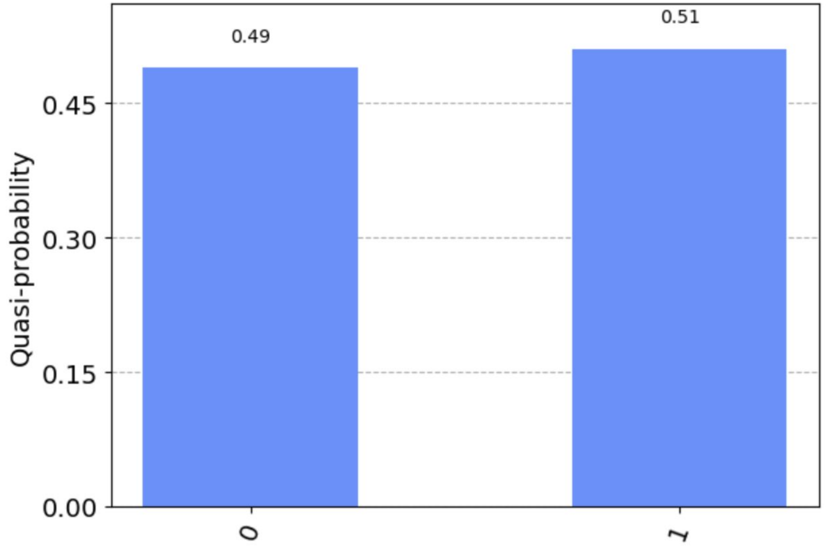
In [11]:
```python
from qiskit import QuantumCircuit

qc = QuantumCircuit(1, 1) # Criando um circuito de 1 qubit e 1 bit
qc.h(0) # Pondo o qubit em uma superposição

qc.measure(0, 0) # Medindo o estado do qubit e armazenando no bit

qc.draw('mpl')
```

Out[11]:



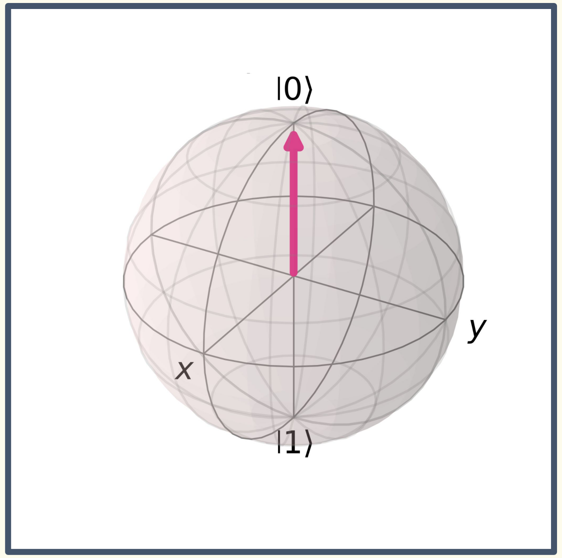
In [12]:
```python
from qiskit import Aer, execute
from qiskit.visualization import plot_distribution

# Simulando o circuito criado como em um computador quântico sem ruído
backend = Aer.get_backend('aer_simulator')
job = execute(qc, backend, shots = 1024)
result = job.result()
counts = result.get_counts()

# Plotando um histograma de probabilidades
plot_distribution(counts)
```

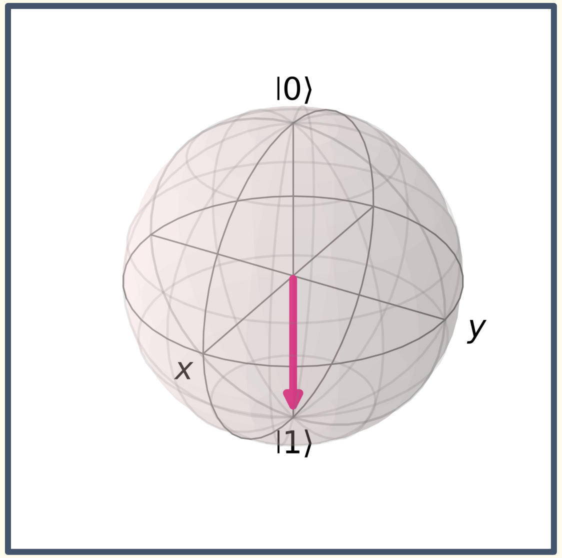
Out[12]:



Esfera de Bloch

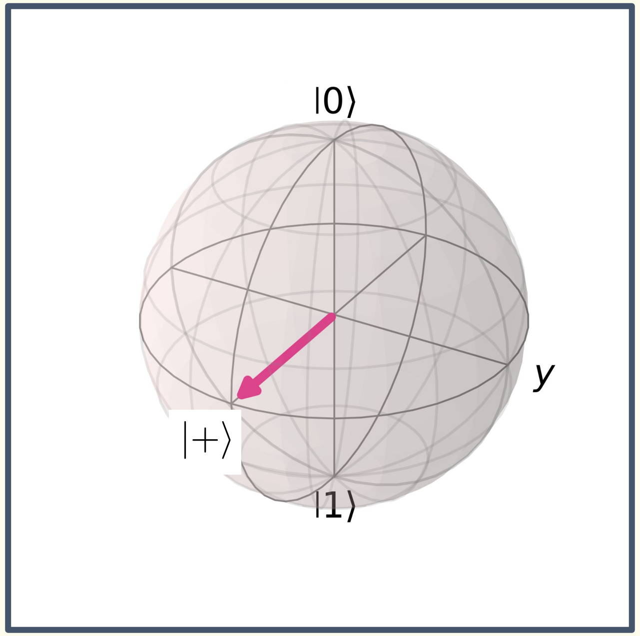
- Uma maneira muito útil de se representar o estado de um qubit é a **esfera de Bloch**
- Colocamos os estados $|0\rangle$ e $|1\rangle$ ao longo do **eixo z** de uma esfera

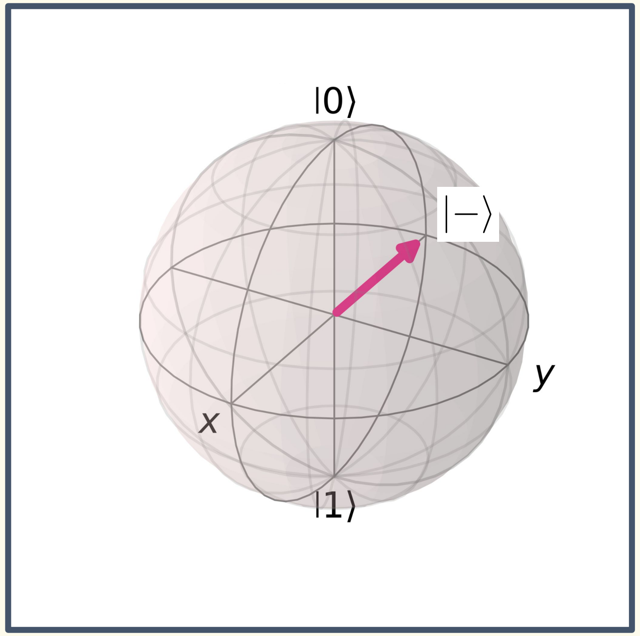




Esfera de Bloch

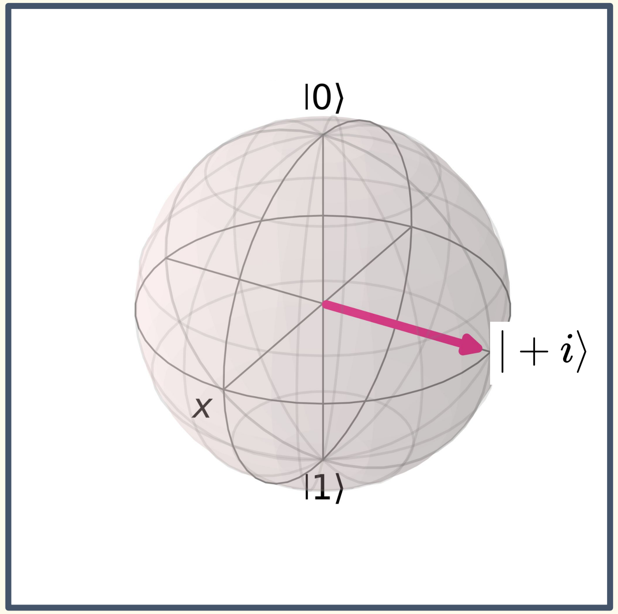
- Uma maneira muito útil de se representar o estado de um qubit é a **esfera de Bloch**
- Os estados $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ficam ao longo do **eixo x**

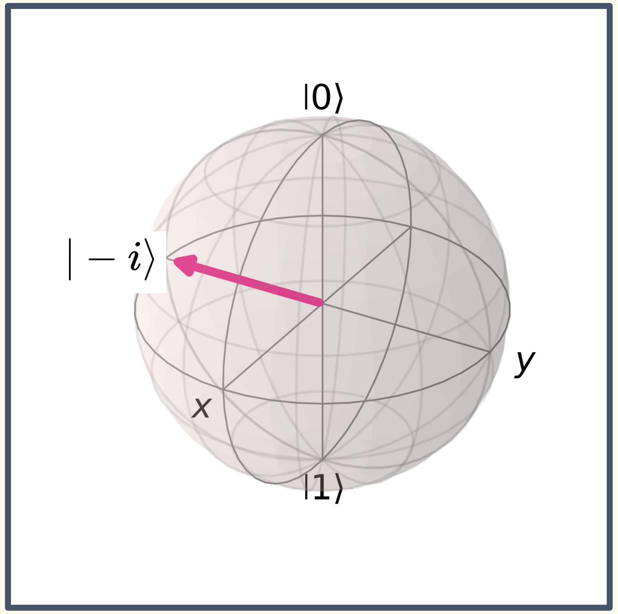




Esfera de Bloch

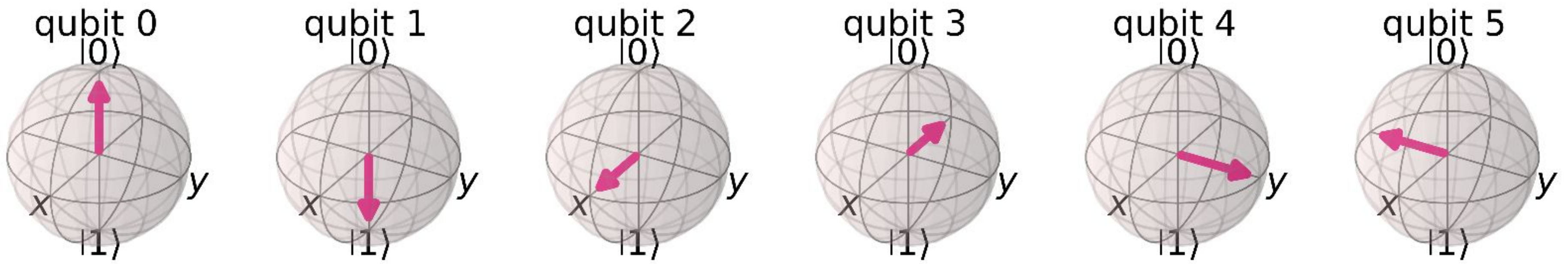
- Uma maneira muito útil de se representar o estado de um qubit é a **esfera de Bloch**
- Os estados $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ e $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ ficam ao longo do **eixo y**





Esfera de Bloch

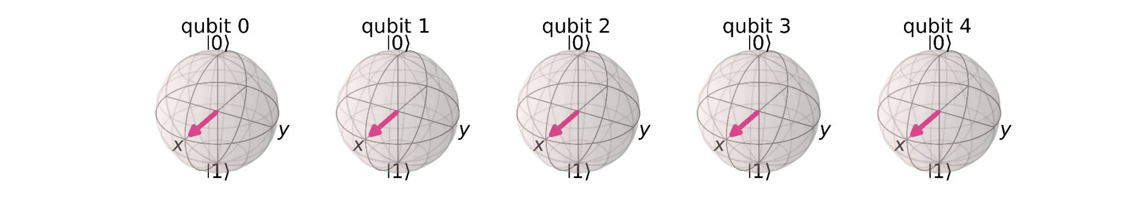
Podemos representar um sistema de vários qubits em várias esferas de Bloch



Esfera de Bloch

Suponha então que fazemos o seguinte experimento:

I. Preparamos 5 qubits, cada um no estado superposto $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$



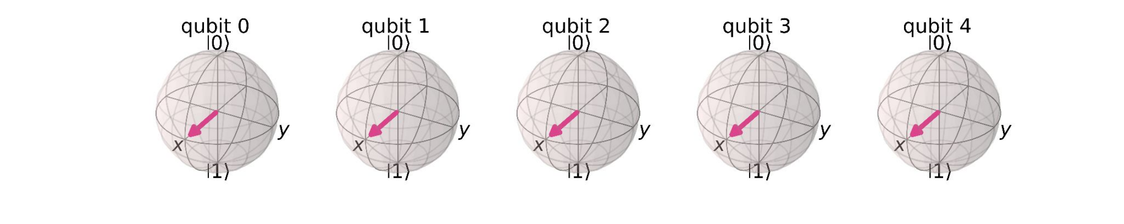
Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$

Esfera de Bloch

Suponha então que fazemos o seguinte experimento:

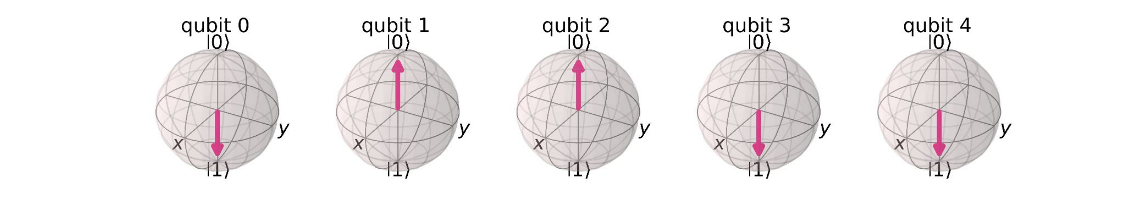
I. Preparamos 5 qubits, cada um no estado superposto $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

II. Medimos cada qubit



Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$

Medição



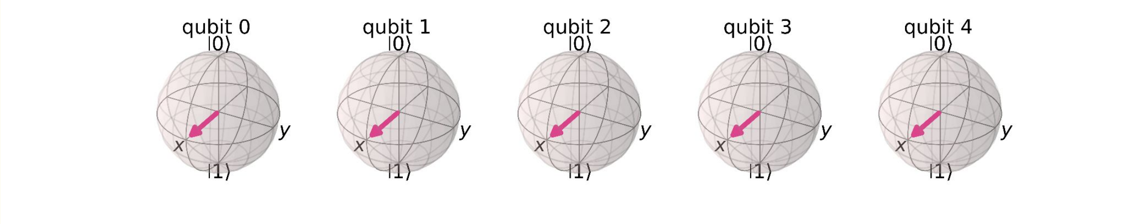
Estado conjunto: $|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle$

Esfera de Bloch

Suponha então que fazemos o seguinte experimento:

I. Preparamos 5 qubits, cada um no estado superposto $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

II. Medimos cada qubit

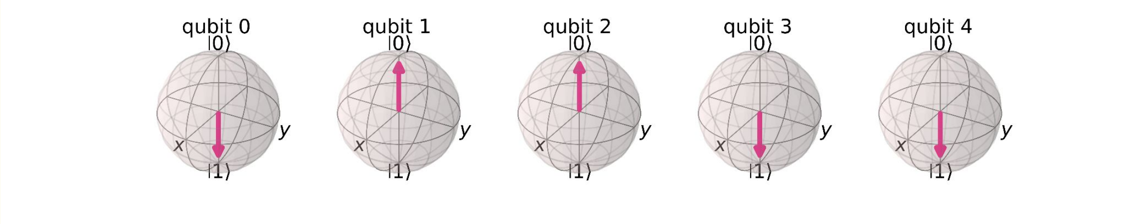


Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$

Medição

Resultado: geramos o número binário 10011 !!

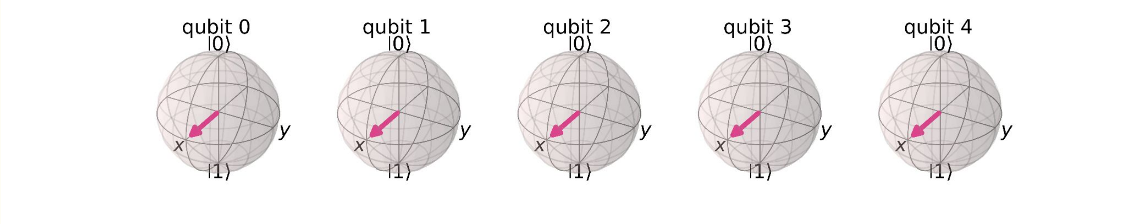
= 38, em decímais



Estado conjunto: $|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle$

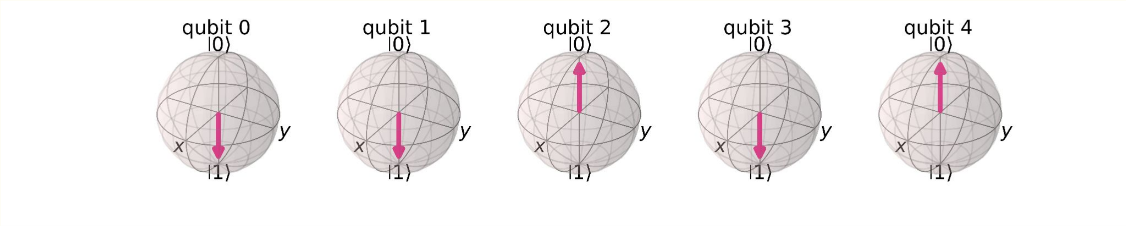
Esfera de Bloch

- Mas **cuidado**: cada qubit colapsa em $|0\rangle$ ou $|1\rangle$ com uma certa **probabilidade**



Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$

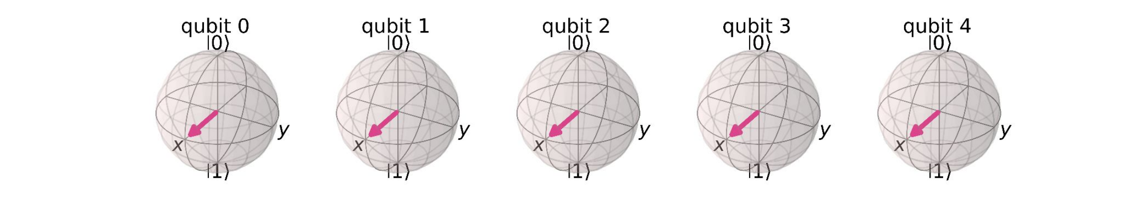
Medição



Estado conjunto: $|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle$

Esfera de Bloch

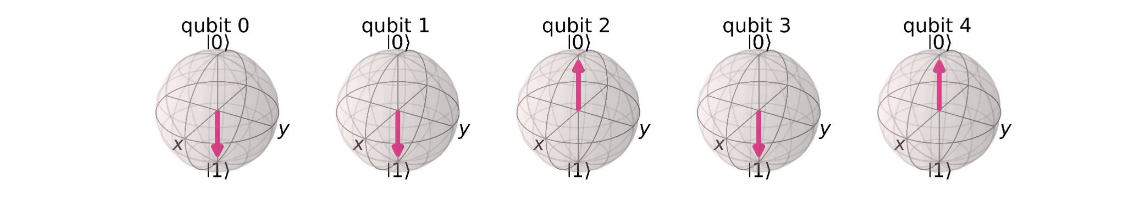
- Mas **cuidado**: cada qubit colapsa em $|0\rangle$ ou $|1\rangle$ com uma certa **probabilidade**
- Logo, se repetimos o **mesmo experimento**, o resultado pode ser **outro número** binário de 5 dígitos



Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$

Resultado: geramos o número binário 11010 !!

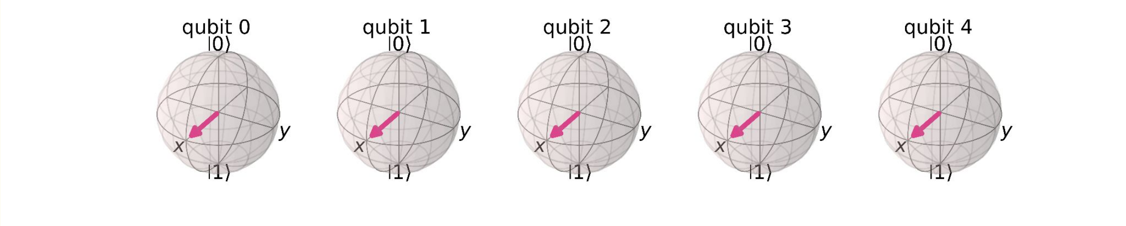
= 50, em decimais



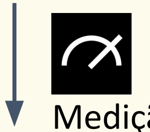
Estado conjunto: $|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle$

Esfera de Bloch

- Para gerar todas as possibilidades podemos repetir o experimento um número muito grande de vezes (1000 por ex.)
  - Experimentalmente, isso pode ser feito em frações de segundos!



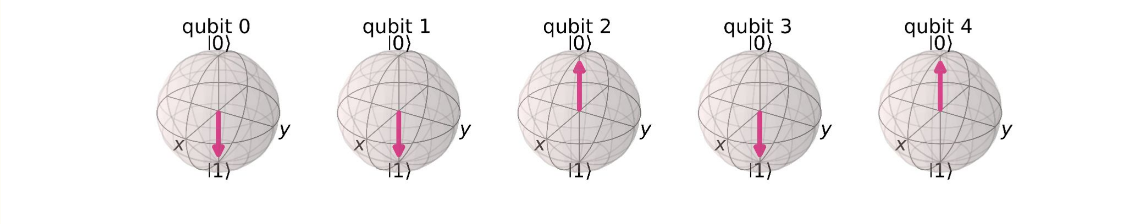
Estado conjunto: $|+\rangle|+\rangle|+\rangle|+\rangle|+\rangle$



Medição

Resultado: geramos o número binário 11010 !!

= 50, em decimais



Estado conjunto: $|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle$

Qiskit | Fall Fest 2023

Esfera de Bloch

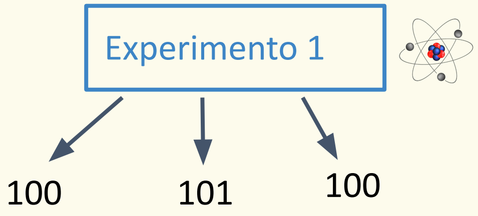
- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110

Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez

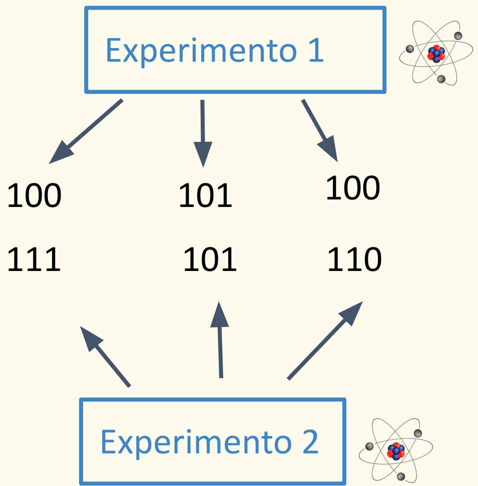
Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez
- Um computador quântico poderia proceder da seguinte forma:



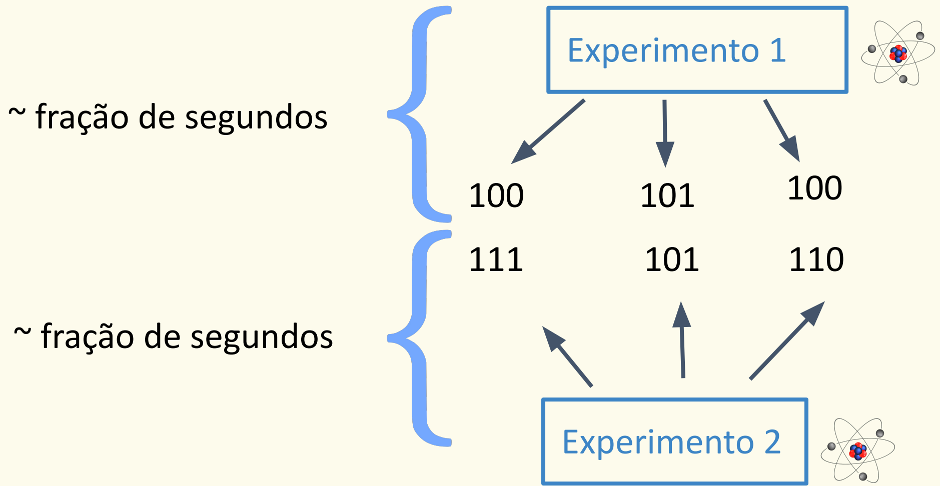
Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez
- Um computador quântico poderia proceder da seguinte forma:



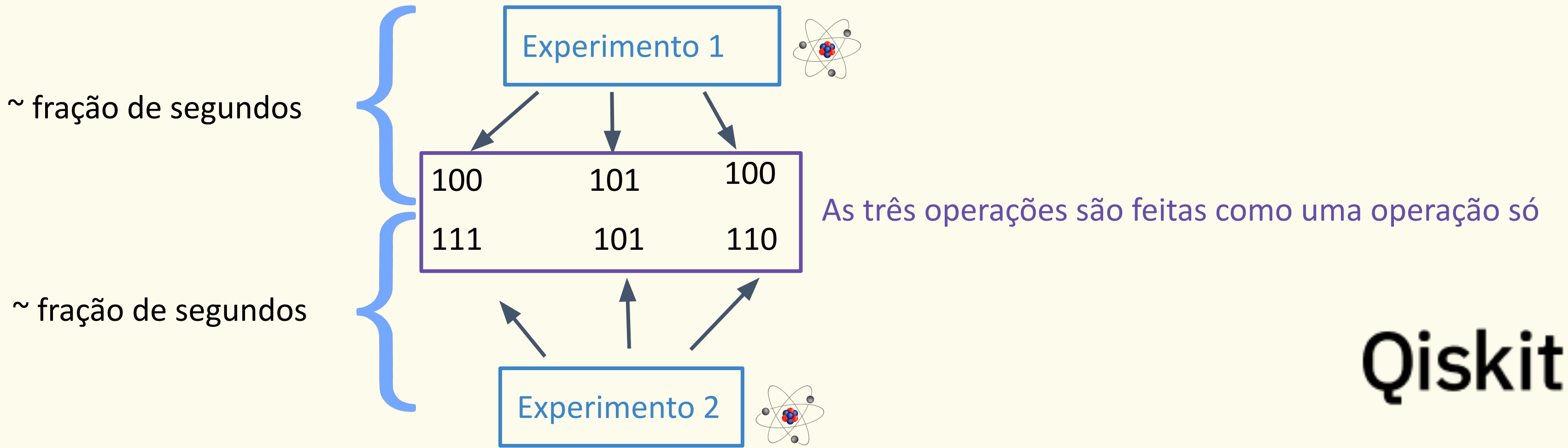
Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez
- Um computador quântico poderia proceder da seguinte forma:



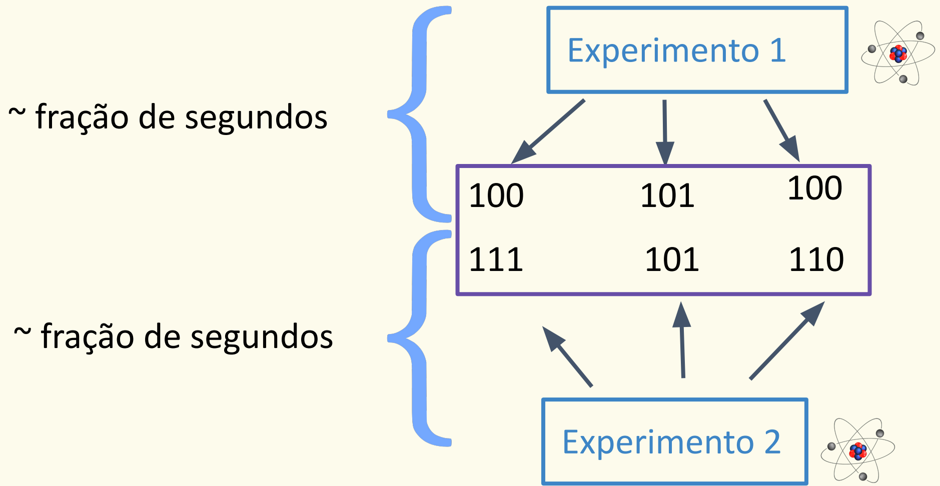
Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez
- Um computador quântico poderia proceder da seguinte forma:



Esfera de Bloch

- Suponha então que queremos calcular as seguintes operações
  - 100 + 111
  - 101 + 101
  - 100 + 110
- Um computador clássico procederia gerando cada número e fazendo uma operação de cada vez
- Um computador quântico poderia proceder da seguinte forma:

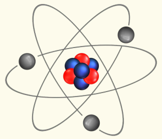


Entretanto, um computador clássico realizaria este exemplo de maneira suficientemente eficiente.

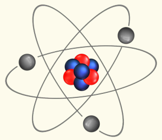
Logo, não há nenhuma grande vantagem em utilizar um computador quântico.

Muitos qubits

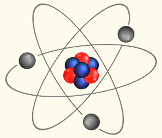
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



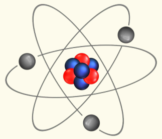
$$|q_1\rangle = |1\rangle$$



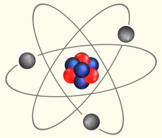
$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

Muitos qubits

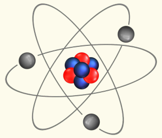
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|q_1\rangle = |1\rangle$$



$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

$$|q_2 q_1 q_0\rangle = |q_2\rangle|q_1\rangle|q_0\rangle$$

Muitos qubits

- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente

$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|q_1\rangle = |1\rangle$$

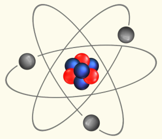
$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

$$|q_2 q_1 q_0\rangle = |q_2\rangle|q_1\rangle|q_0\rangle$$

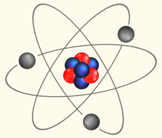
$$= \left(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle\right).\,|1\rangle.\,\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Muitos qubits

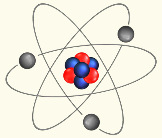
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|q_1\rangle = |1\rangle$$

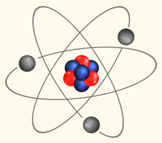


$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

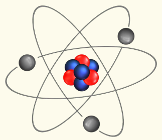
$$\begin{aligned}|q_2 q_1 q_0\rangle &= |q_2\rangle|q_1\rangle|q_0\rangle \\ &= \left(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle\right). |1\rangle. \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \left(\sqrt{\tfrac{2}{3}}|0\rangle|1\rangle + \sqrt{\tfrac{1}{3}}|1\rangle|1\rangle\right). \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\end{aligned}$$

Muitos qubits

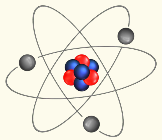
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|q_1\rangle = |1\rangle$$

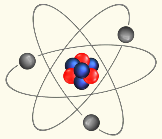


$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

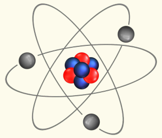
$$\begin{aligned}
|q_2 q_1 q_0\rangle &= |q_2\rangle|q_1\rangle|q_0\rangle \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle\right).\,|1\rangle.\,\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle|1\rangle + \sqrt{\tfrac{1}{3}}|1\rangle|1\rangle\right).\,\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&\boxed{= \sqrt{\tfrac{1}{3}}|0\rangle|1\rangle|0\rangle + \sqrt{\tfrac{1}{3}}|0\rangle|1\rangle|1\rangle + \tfrac{1}{\sqrt{6}}|1\rangle|1\rangle|0\rangle + \tfrac{1}{\sqrt{6}}|1\rangle|1\rangle|1\rangle}
\end{aligned}$$

Muitos qubits

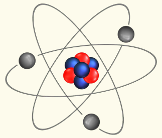
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|q_1\rangle = |1\rangle$$



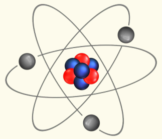
$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

Convenção do Qiskit

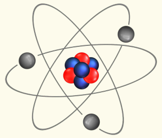
$$\begin{aligned}
|q_2 q_1 q_0\rangle &= |q_2\rangle|q_1\rangle|q_0\rangle \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle\right).|1\rangle.\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle|1\rangle + \sqrt{\tfrac{1}{3}}|1\rangle|1\rangle\right).\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \sqrt{\frac{1}{3}}|0\rangle|1\rangle|0\rangle + \sqrt{\frac{1}{3}}|0\rangle|1\rangle|1\rangle \\
&\quad + \frac{1}{\sqrt{6}}|1\rangle|1\rangle|0\rangle + \frac{1}{\sqrt{6}}|1\rangle|1\rangle|1\rangle
\end{aligned}$$

Muitos qubits

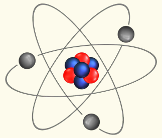
- Podemos organizar o estado de um sistema de vários qubits "multiplicando" cada estado linearmente



$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|q_1\rangle = |1\rangle$$



$$|q_2\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

$$\begin{aligned}
|q_2 q_1 q_0\rangle &= |q_2\rangle|q_1\rangle|q_0\rangle \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle\right).\,|1\rangle.\,\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \left(\sqrt{\tfrac{2}{3}}|0\rangle|1\rangle + \sqrt{\tfrac{1}{3}}|1\rangle|1\rangle\right).\,\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \sqrt{\tfrac{1}{3}}|010\rangle + \sqrt{\tfrac{1}{3}}|011\rangle + \tfrac{1}{\sqrt{6}}|110\rangle + \tfrac{1}{\sqrt{6}}|111\rangle
\end{aligned}$$

Muitos qubits

- De maneira geral, o **estado composto** de um sistema de N qubits nos estados $|q_0\rangle$, $|q_1\rangle$, $|q_2\rangle$, ..., $|q_N\rangle$ é dado por

$$|q_N\rangle \dots |q_2\rangle|q_1\rangle|q_0\rangle \equiv |q_N \dots q_2 q_1 q_0\rangle$$

A "ordem reversa" é uma convenção

Por exemplo:

$$|q_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|q_1\rangle = |1\rangle$$

$$\longrightarrow \quad |q_1 q_0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

Muitos qubits

- De maneira geral, o **estado composto** de um sistema de N qubits nos estados $|q_0\rangle$, $|q_1\rangle$, $|q_2\rangle$, ..., $|q_N\rangle$ é dado por

$$|q_N\rangle \dots |q_2\rangle|q_1\rangle|q_0\rangle \equiv |q_N \dots q_2 q_1 q_0\rangle$$

Muitos qubits

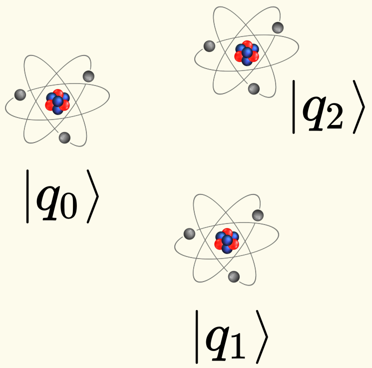
- De maneira geral, o **estado composto** de um sistema de N qubits nos estados $|q_0\rangle$, $|q_1\rangle$, $|q_2\rangle$, ..., $|q_N\rangle$ é dado por

$$|q_N\rangle \ldots |q_2\rangle |q_1\rangle |q_0\rangle \equiv |q_N \ldots q_2 q_1 q_0\rangle$$

A "ordem reversa" é uma convenção

Muitos qubits

A generalização da **regra de Born** é intuitiva:



$$|q_2 q_1 q_0\rangle = \sqrt{\frac{1}{3}}|010\rangle + \sqrt{\frac{1}{3}}|011\rangle + \frac{1}{\sqrt{6}}|110\rangle + \frac{1}{\sqrt{6}}|111\rangle$$

Probabilidade ⅓ de medir 010

Probabilidade ⅓ de medir 011

Probabilidade ⅙ de medir 110

Probabilidade ⅙ de medir 111

Emaranhamento

- Uma das coisas mais malucas da MQ é que existem certos vetores de estado de sistemas compostos que **não são separáveis**

Emaranhamento

- Uma das coisas mais malucas da MQ é que existem certos vetores de estado de sistemas compostos que **não são separáveis**

- Como assim?
    - Considere, por exemplo, um sistema de dois qubits no estado

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Emaranhamento

- Uma das coisas mais malucas da MQ é que existem certos vetores de estado de sistemas compostos que **não são separáveis**

- Como assim?
  - Considere, por exemplo, um sistema de dois qubits no estado

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

  - Agora tente encontrar a, b, c e d tais que

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$$

Emaranhamento

- Uma das coisas mais malucas da MQ é que existem certos vetores de estado de sistemas compostos que **não são separáveis**

- Como assim?
  - Considere, por exemplo, um sistema de dois qubits no estado

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

  - Agora tente encontrar a, b, c e d tais que

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \longrightarrow \begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases}$$

Emaranhamento

- Uma das coisas mais malucas da MQ é que existem certos vetores de estado de sistemas compostos que **não são separáveis**

- Como assim?
  - Considere, por exemplo, um sistema de dois qubits no estado

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

  - Agora tente encontrar a, b, c e d tais que

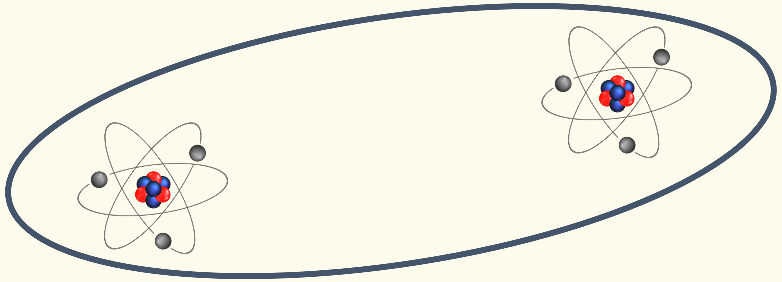
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \longrightarrow \begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases}$$

Sistema sem solução!

Emaranhamento

- Conclusão: **não existem** estados $|q_0\rangle$, $|q_1\rangle$ tais que

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |q_1\rangle|q_0\rangle$$



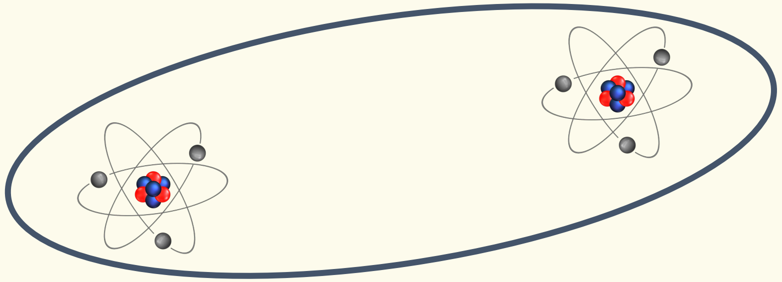
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Emaranhamento

- Conclusão: **não existem** estados $|q_0\rangle$, $|q_1\rangle$ tais que

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |q_1\rangle|q_0\rangle$$

- Em outras palavras, não existe o estado de cada qubit separadamente. Os dois qubits estão **emaranhados**



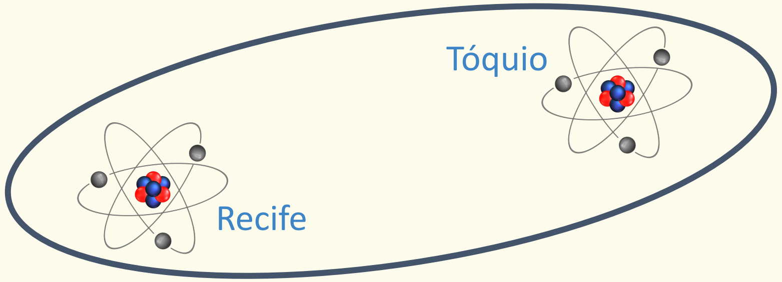
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Emaranhamento

- Conclusão: **não existem** estados $|q_0\rangle$, $|q_1\rangle$ tais que

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |q_1\rangle|q_0\rangle$$

- Em outras palavras, não existe o estado de cada qubit separadamente. Os dois qubits estão **emaranhados**



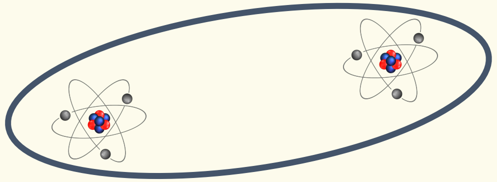
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Emaranhamento

- Os exemplos mais famosos de estados emaranhados são os **estados de Bell**

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

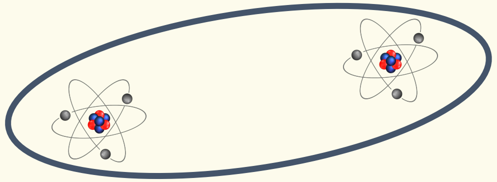
Emaranhamento

- Os exemplos mais famosos de estados emaranhados são os **estados de Bell**

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Aplicações mais importantes:
  - Teleporte quântico (possível simular com Qiskit)
  - Criptografia
  - Computação quântica! **Yey!**



$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Conclusão

- Bits vs Qubits
  - Bit: 0, 1
  - Qubit: 0, 1, qualquer combinação linear de 0 e 1

Conclusão

- Bits vs Qubits
  - Bit: 0, 1
  - Qubit: 0, 1, qualquer combinação linear de 0 e 1

- Sistemas quânticos podem estar em estados **superpostos**

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \ldots$$

Conclusão

- Bits vs Qubits
  - Bit: 0, 1
  - Qubit: 0, 1, qualquer combinação linear de 0 e 1

- Sistemas quânticos podem estar em estados **superpostos**

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \dots$$

- **Regra de Born:** a medição colapsa o sistema no estado $|i\rangle$ com probabilidade $|a_i|^2$

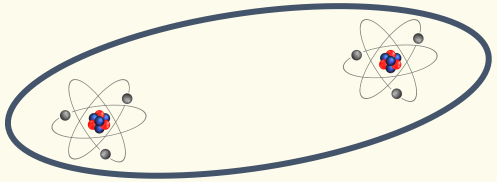
Ex. $|q\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \longrightarrow$

$|0\rangle$ Com probabilidade $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

$|1\rangle$ Com probabilidade $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

Conclusão

- Sistemas compostos podem estar em estados **emaranhados**!



$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Thank you