

Introdução à Computação Quântica

MOUTA Leonardo

PFC-F - ITA/ISAE-SUPAERO



June 1, 2022

Objetivo: Descrever os princípios de funcionamento da computação quântica

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

- 1 **Motivação**
- 2 **Sistemas de Um Qubit**
 - Formalismo
 - Representação
- 3 **Sistemas de Múltiplos Qubits**
 - Formalismo
 - Representação
- 4 **Operações Computacionais**
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 **Exemplos Ilustrativos**
 - Estados Entrelaçados
 - Protocolo de Teletransporte

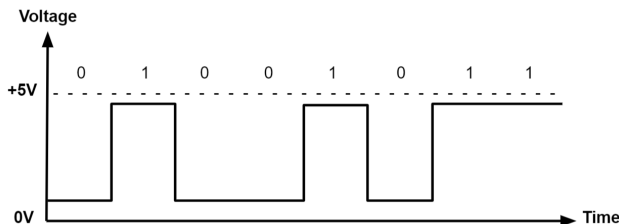
Na computação clássica, representamos os sinais (digitais) como uma combinação de “uns” e “zeros”, cujos valores são associados a alguma grandeza física (voltagem, corrente, etc.).

Na computação clássica, representamos os sinais (digitais) como uma combinação de “uns” e “zeros”, cujos valores são associados a alguma grandeza física (voltagem, corrente, etc.).

Em cima desses sinais binários, o computador realiza suas operações.

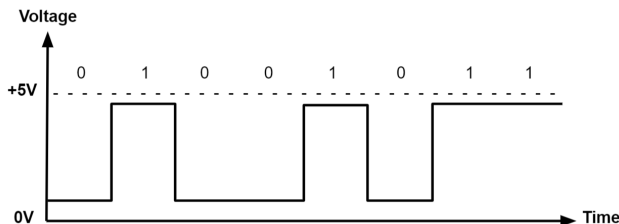
Na computação clássica, representamos os sinais (digitais) como uma combinação de “uns” e “zeros”, cujos valores são associados a alguma grandeza física (voltagem, corrente, etc.).

Em cima desses sinais binários, o computador realiza suas operações.



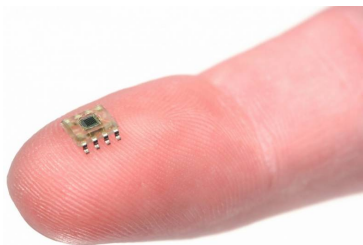
Na computação clássica, representamos os sinais (digitais) como uma combinação de “uns” e “zeros”, cujos valores são associados a alguma grandeza física (voltagem, corrente, etc.).

Em cima desses sinais binários, o computador realiza suas operações.

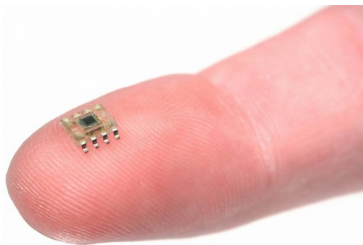


Em um computador clássico, um sinal só pode ser ou zero ou um em um determinado momento!

A miniaturização do hardware trouxe a mecânica quântica para a fabricação de computadores, mas o funcionamento da computação clássica ainda é o mesmo: **operações determinísticas em cima de sinais digitais binários.**



A miniaturização do hardware trouxe a mecânica quântica para a fabricação de computadores, mas o funcionamento da computação clássica ainda é o mesmo: **operações determinísticas em cima de sinais digitais binários.**

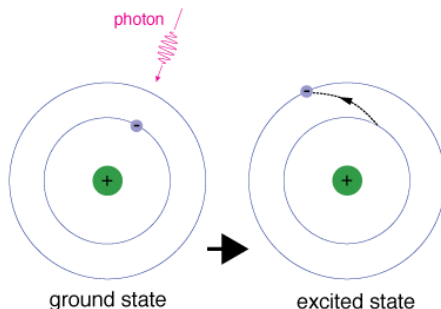


E se a mecânica quântica fosse usada nas operações do computador?

Considere que o “zero” e o “um” estão agora associados a uma grandeza física regida pela mecânica quântica: o spin de um elétron, a polarização de um fóton, a excitação de um átomo, etc.

Considere que o “zero” e o “um” estão agora associados a uma grandeza física regida pela mecânica quântica: o spin de um elétron, a polarização de um fóton, a excitação de um átomo, etc.

Exemplo: imagine que o estado fundamental de um átomo representa “zero” e o estado excitado do mesmo átomo representa “um”. Isso é um “bit quântico”:



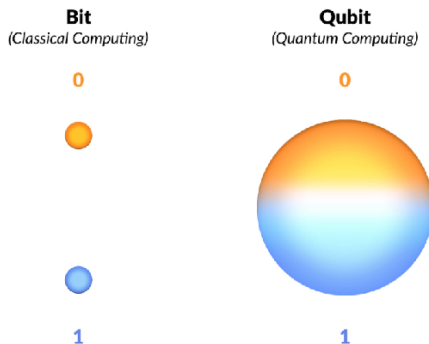
Diferentemente dos bits clássicos, bits quânticos existem em uma superposição dos estados “zero” e “um”.

Diferentemente dos bits clássicos, bits quânticos existem em uma superposição dos estados “zero” e “um”.

É apenas após a realização de uma medida que esse estado superposto colapsa em um dos estados base.

Diferentemente dos bits clássicos, bits quânticos existem em uma superposição dos estados “zero” e “um”.

É apenas após a realização de uma medida que esse estado superposto colapsa em um dos estados base.



Conhecemos apenas algumas vantagens da computação quântica:

Conhecemos apenas algumas vantagens da computação quântica:

- Redução na complexidade de certos problemas

Conhecemos apenas algumas vantagens da computação quântica:

- Redução na complexidade de certos problemas
- Ganho de velocidade

Conhecemos apenas algumas vantagens da computação quântica:

- Redução na complexidade de certos problemas
- Ganho de velocidade
- Execução de simulações complexas

Conhecemos apenas algumas vantagens da computação quântica:

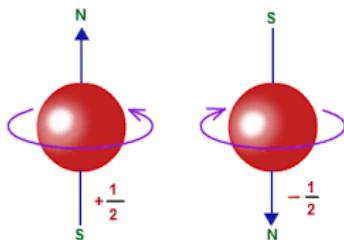
- Redução na complexidade de certos problemas
- Ganho de velocidade
- Execução de simulações complexas

Mas a verdade é que não temos ideia do verdadeiro potencial da computação quântica!

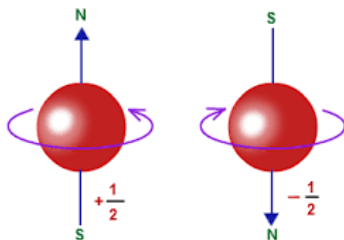
- 1 Motivação
- 2 **Sistemas de Um Qubit**
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Considere, por exemplo, um único elétron. Sabemos que o spin desse elétron pode ser do tipo “up” ou “down”. Conseguimos medir o spin “up” ou “down” experimentalmente (Stern–Gerlach).



Considere, por exemplo, um único elétron. Sabemos que o spin desse elétron pode ser do tipo “up” ou “down”. Conseguimos medir o spin “up” ou “down” experimentalmente (Stern–Gerlach).



Vamos definir o spin “up” como representando o estado $|0\rangle$ e o spin “down” como representando o estado $|1\rangle$.

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

→ “Computacional” porque esses são estados que conseguimos medir fisicamente (spins “up” e “down”)

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

→ “Computacional” porque esses são estados que conseguimos medir fisicamente (spins “up” e “down”)

→ “Base” porque qualquer estado $|\psi\rangle$ do elétron pode ser escrito como uma superposição desses dois estados:

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

→ “Computacional” porque esses são estados que conseguimos medir fisicamente (spins “up” e “down”)

→ “Base” porque qualquer estado $|\psi\rangle$ do elétron pode ser escrito como uma superposição desses dois estados:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Com $a_0, a_1 \in \mathbb{C}$. Além disso, em um experimento, só podemos medir os estados $|0\rangle$ ou $|1\rangle$. Pela regra de Born, torna-se necessário:

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

→ “Computacional” porque esses são estados que conseguimos medir fisicamente (spins “up” e “down”)

→ “Base” porque qualquer estado $|\psi\rangle$ do elétron pode ser escrito como uma superposição desses dois estados:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Com $a_0, a_1 \in \mathbb{C}$. Além disso, em um experimento, só podemos medir os estados $|0\rangle$ ou $|1\rangle$. Pela regra de Born, torna-se necessário:

$$|a_0|^2 + |a_1|^2 = 1$$

Os estados $|0\rangle$, $|1\rangle$ são a chamada “**base computacional**”:

→ “Computacional” porque esses são estados que conseguimos medir fisicamente (spins “up” e “down”)

→ “Base” porque qualquer estado $|\psi\rangle$ do elétron pode ser escrito como uma superposição desses dois estados:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Com $a_0, a_1 \in \mathbb{C}$. Além disso, em um experimento, só podemos medir os estados $|0\rangle$ ou $|1\rangle$. Pela regra de Born, torna-se necessário:

$$|a_0|^2 + |a_1|^2 = 1$$

Os possíveis valores de $|\psi\rangle$ são um **qubit**.

Os estados/vetores $|0\rangle$ e $|1\rangle$ formam uma base do espaço vetorial complexo V ao qual pertence o qubit $|\psi\rangle$. Além disso, essa base é ortonormal:

Os estados/vetores $|0\rangle$ e $|1\rangle$ formam uma base do espaço vetorial complexo V ao qual pertence o qubit $|\psi\rangle$. Além disso, essa base é ortonormal:

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

Observação: para fins de mecânica quântica, toda base de V deve ser ortonormal!

Os estados/vetores $|0\rangle$ e $|1\rangle$ formam uma base do espaço vetorial complexo V ao qual pertence o qubit $|\psi\rangle$. Além disso, essa base é ortonormal:

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

Observação: para fins de mecânica quântica, toda base de V deve ser ortonormal!

A escolha de uma base permite escrever um estado $|\psi\rangle$ em forma matricial:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

Os estados/vetores $|0\rangle$ e $|1\rangle$ formam uma base do espaço vetorial complexo V ao qual pertence o qubit $|\psi\rangle$. Além disso, essa base é ortonormal:

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

Observação: para fins de mecânica quântica, toda base de V deve ser ortonormal!

A escolha de uma base permite escrever um estado $|\psi\rangle$ em forma matricial:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

Doravante, a menos que especificado, sempre iremos escrever os qubits (e seus operadores) em relação à base $\{|0\rangle, |1\rangle\}$.

Alguns valores particulares de a_0, a_1 levam a valores de $|\psi\rangle$ que recebem nomes especiais:

Alguns valores particulares de a_0, a_1 levam a valores de $|\psi\rangle$ que recebem nomes especiais:

① Estados $|+\rangle$ e $|-\rangle$

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

Alguns valores particulares de a_0, a_1 levam a valores de $|\psi\rangle$ que recebem nomes especiais:

1 Estados $|+\rangle$ e $|-\rangle$

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

2 Estados $|+i\rangle$ e $|-i\rangle$

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

Alguns valores particulares de a_0, a_1 levam a valores de $|\psi\rangle$ que recebem nomes especiais:

① Estados $|+\rangle$ e $|-\rangle$

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

② Estados $|+i\rangle$ e $|-i\rangle$

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

Os estados $\{|+\rangle, |-\rangle\}$ e $\{|+i\rangle, |-i\rangle\}$ formam bases ortonormais de V .

Alguns valores particulares de a_0, a_1 levam a valores de $|\psi\rangle$ que recebem nomes especiais:

❶ Estados $|+\rangle$ e $|-\rangle$

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

❷ Estados $|+i\rangle$ e $|-i\rangle$

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

Os estados $\{|+\rangle, |-\rangle\}$ e $\{|+i\rangle, |-i\rangle\}$ formam bases ortonormais de V .

A base $\{|+\rangle, |-\rangle\}$, chamada “base de Hadamard”, é particularmente importante em circuitos quânticos.

Em um qubit, um estado é sempre da forma:

Em um qubit, um estado é sempre da forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Em um qubit, um estado é sempre da forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Pela regra de Born, temos as probabilidades de medir cada estado:

Em um qubit, um estado é sempre da forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Pela regra de Born, temos as probabilidades de medir cada estado:

$$\begin{cases} P(|0\rangle) = |a_0|^2 \\ P(|1\rangle) = |a_1|^2 \end{cases}$$

Em um qubit, um estado é sempre da forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Pela regra de Born, temos as probabilidades de medir cada estado:

$$\begin{cases} P(|0\rangle) = |a_0|^2 \\ P(|1\rangle) = |a_1|^2 \end{cases}$$

Uma medição em qubit se converte em um bit clássico de forma direta:

Em um qubit, um estado é sempre da forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Pela regra de Born, temos as probabilidades de medir cada estado:

$$\begin{cases} P(|0\rangle) = |a_0|^2 \\ P(|1\rangle) = |a_1|^2 \end{cases}$$

Uma medição em qubit se converte em um bit clássico de forma direta:

$$\begin{cases} |0\rangle \rightarrow 0 \\ |1\rangle \rightarrow 1 \end{cases}$$

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

$$|\psi\rangle = e^{i\alpha}|\psi'\rangle$$

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

$$|\psi\rangle = e^{i\alpha}|\psi'\rangle$$

O valor α é a chamada “fase global”. Em geral, a fase global de um qubit é irrelevante (há exceções).

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

$$|\psi\rangle = e^{i\alpha}|\psi'\rangle$$

O valor α é a chamada “fase global”. Em geral, a fase global de um qubit é irrelevante (há exceções).

Considerando uma transformação de fase global, podemos escrever qualquer qubit como:

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

$$|\psi\rangle = e^{i\alpha}|\psi'\rangle$$

O valor α é a chamada “fase global”. Em geral, a fase global de um qubit é irrelevante (há exceções).

Considerando uma transformação de fase global, podemos escrever qualquer qubit como:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

Considere o número complexo de módulo unitário $e^{i\alpha}$, com $\alpha \in [0, 2\pi)$. Dizemos que dois qubits $|\psi\rangle, |\psi'\rangle$ são equivalentes se existe α tal que:

$$|\psi\rangle = e^{i\alpha}|\psi'\rangle$$

O valor α é a chamada “fase global”. Em geral, a fase global de um qubit é irrelevante (há exceções).

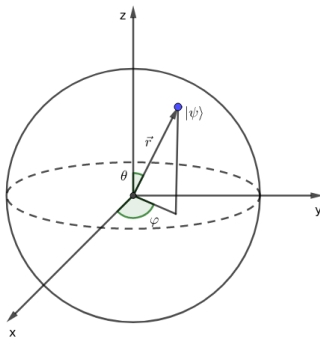
Considerando uma transformação de fase global, podemos escrever qualquer qubit como:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

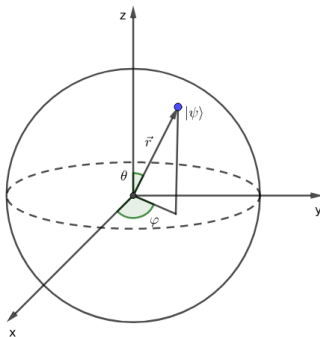
Com $\theta \in [0, \pi]$ e $\varphi \in [0, 2\pi)$. O valor φ é a “fase relativa”.

Considerando a forma do qubit apresentada no slide anterior, vemos que um estado $|\psi\rangle$ pode ser plotado em uma esfera de raio unitário em função dos parâmetros (θ, φ) , que parametrizam a esfera:

Considerando a forma do qubit apresentada no slide anterior, vemos que um estado $|\psi\rangle$ pode ser plotado em uma esfera de raio unitário em função dos parâmetros (θ, φ) , que parametrizam a esfera:



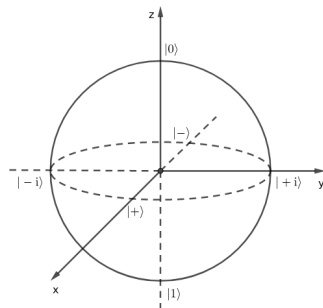
Considerando a forma do qubit apresentada no slide anterior, vemos que um estado $|\psi\rangle$ pode ser plotado em uma esfera de raio unitário em função dos parâmetros (θ, φ) , que parametrizam a esfera:



Matematicamente $\vec{r} = [\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta]^T$

Considerando os pontos notórios definidos previamente, vemos que eles são “especiais” na esfera de Bloch:

- $|0\rangle \rightarrow (0, 0, 1)$
- $|1\rangle \rightarrow (0, 0, -1)$
- $|+\rangle \rightarrow (1, 0, 0)$
- $|-\rangle \rightarrow (-1, 0, 0)$
- $|+i\rangle \rightarrow (0, 1, 0)$
- $|-i\rangle \rightarrow (0, -1, 0)$



- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Considere agora, por exemplo, dois elétrons, A e B. Em cada um temos um estado diferente:

Considere agora, por exemplo, dois elétrons, A e B. Em cada um temos um estado diferente:

$$\begin{cases} |\phi\rangle_A = a_0|0\rangle_A + a_1|1\rangle_A \\ |\phi\rangle_B = b_0|0\rangle_B + b_1|1\rangle_B \end{cases}$$

Considere agora, por exemplo, dois elétrons, A e B. Em cada um temos um estado diferente:

$$\begin{cases} |\phi\rangle_A = a_0|0\rangle_A + a_1|1\rangle_A \\ |\phi\rangle_B = b_0|0\rangle_B + b_1|1\rangle_B \end{cases}$$

Representamos o sistema completo usando o produto tensorial:

$$\begin{aligned} |\phi\rangle_{AB} = |\phi\rangle_A \otimes |\phi\rangle_B = & a_0b_0|0\rangle_A \otimes |0\rangle_B \\ & + a_0b_1|0\rangle_A \otimes |1\rangle_B \\ & + a_1b_0|1\rangle_A \otimes |0\rangle_B \\ & + a_1b_1|1\rangle_A \otimes |1\rangle_B \end{aligned}$$

Em um sistema de n qubits, cada qubit i representa um espaço vetorial complexo V_i de base computacional $\{|0\rangle_i, |1\rangle_i\}$. A base computacional para o sistema completo $V = V_{n-1} \otimes \dots \otimes V_0$ é intuitiva:

Em um sistema de n qubits, cada qubit i representa um espaço vetorial complexo V_i de base computacional $\{|0\rangle_i, |1\rangle_i\}$. A base computacional para o sistema completo $V = V_{n-1} \otimes \dots \otimes V_0$ é intuitiva:

$$B(V) = \{|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0, |0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |1\rangle_0, \dots\}$$

Em um sistema de n qubits, cada qubit i representa um espaço vetorial complexo V_i de base computacional $\{|0\rangle_i, |1\rangle_i\}$. A base computacional para o sistema completo $V = V_{n-1} \otimes \dots \otimes V_0$ é intuitiva:

$$B(V) = \{|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0, |0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |1\rangle_0, \dots\}$$

Observação: a ordem dos qubits no produto tensorial não é fundamental, desde que seja mantida de forma coerente.

Em um sistema de n qubits, cada qubit i representa um espaço vetorial complexo V_i de base computacional $\{|0\rangle_i, |1\rangle_i\}$. A base computacional para o sistema completo $V = V_{n-1} \otimes \dots \otimes V_0$ é intuitiva:

$$B(V) = \{|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0, |0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |1\rangle_0, \dots\}$$

Observação: a ordem dos qubits no produto tensorial não é fundamental, desde que seja mantida de forma coerente.

Ignorando a notação custosa do produto tensorial...

$$B(V) = \{|0\rangle_{n-1} \dots |0\rangle_1 |0\rangle_0, |0\rangle_{n-1} \dots |0\rangle_1 |1\rangle_0, \dots\}$$

Em um sistema de n qubits, cada qubit i representa um espaço vetorial complexo V_i de base computacional $\{|0\rangle_i, |1\rangle_i\}$. A base computacional para o sistema completo $V = V_{n-1} \otimes \dots \otimes V_0$ é intuitiva:

$$B(V) = \{|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0, |0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |1\rangle_0, \dots\}$$

Observação: a ordem dos qubits no produto tensorial não é fundamental, desde que seja mantida de forma coerente.

Ignorando a notação custosa do produto tensorial...

$$B(V) = \{|0\rangle_{n-1} \dots |0\rangle_1 |0\rangle_0, |0\rangle_{n-1} \dots |0\rangle_1 |1\rangle_0, \dots\}$$

Ou melhor ainda:

$$B(V) = \{|0\dots 00\rangle, |0\dots 01\rangle, |0\dots 10\rangle, |0\dots 11\rangle, \dots, |1\dots 11\rangle\}$$

Observação: essa base às vezes é escrita na sua forma decimal

Considerando um sistema de n qubits, podemos escrever qualquer estado na base computacional como:

Considerando um sistema de n qubits, podemos escrever qualquer estado na base computacional como:

$$|\psi\rangle = \sum_{i=0}^{n-1} a_i |i_{bin}\rangle$$

Considerando um sistema de n qubits, podemos escrever qualquer estado na base computacional como:

$$|\psi\rangle = \sum_{i=0}^{n-1} a_i |i_{bin}\rangle$$

Pela regra de Born, a probabilidade de medir o estado $|j_{bin}\rangle$ é:

Considerando um sistema de n qubits, podemos escrever qualquer estado na base computacional como:

$$|\psi\rangle = \sum_{i=0}^{n-1} a_i |i_{bin}\rangle$$

Pela regra de Born, a probabilidade de medir o estado $|j_{bin}\rangle$ é:

$$P(|j_{bin}\rangle) = |\langle j_{bin} | \psi \rangle|^2 = |a_j|^2$$

Considerando um sistema de n qubits, podemos escrever qualquer estado na base computacional como:

$$|\psi\rangle = \sum_{i=0}^{n-1} a_i |i_{bin}\rangle$$

Pela regra de Born, a probabilidade de medir o estado $|j_{bin}\rangle$ é:

$$P(|j_{bin}\rangle) = |\langle j_{bin} | \psi \rangle|^2 = |a_j|^2$$

Medir o estado $|b_{n-1}b_{n-2}\dots b_1b_0\rangle$, $b_i \in \{0, 1\}$ significa medir $|b_{n-1}\rangle$ no qubit $n-1$, $|b_{n-2}\rangle$ no qubit $n-2$, etc.

Todo estado de um sistema de n qubits pode ser escrito como:

Todo estado de um sistema de n qubits pode ser escrito como:

$$|\psi\rangle = a_{n-1}|1\dots 11\rangle + \dots + a_1|0\dots 1\rangle + a_0|0\dots 00\rangle$$

Todo estado de um sistema de n qubits pode ser escrito como:

$$|\psi\rangle = a_{n-1}|1\dots 11\rangle + \dots + a_1|0\dots 1\rangle + a_0|0\dots 00\rangle$$

Mas nem todo estado pode ser decomposto em um produto tensorial nos qubits originais:

Todo estado de um sistema de n qubits pode ser escrito como:

$$|\psi\rangle = a_{n-1}|1\dots 11\rangle + \dots + a_1|0\dots 1\rangle + a_0|0\dots 00\rangle$$

Mas nem todo estado pode ser decomposto em um produto tensorial nos qubits originais:

$$|\psi\rangle = |\psi_{n-1}\rangle_{n-1} \otimes \dots \otimes |\psi_1\rangle_1 \otimes |\psi_0\rangle_0$$

Todo estado de um sistema de n qubits pode ser escrito como:

$$|\psi\rangle = a_{n-1}|1\dots 11\rangle + \dots + a_1|0\dots 1\rangle + a_0|0\dots 00\rangle$$

Mas nem todo estado pode ser decomposto em um produto tensorial nos qubits originais:

$$|\psi\rangle = |\psi_{n-1}\rangle_{n-1} \otimes \dots \otimes |\psi_1\rangle_1 \otimes |\psi_0\rangle_0$$

Quando um estado **não** pode ser decomposto no produto tensorial dos qubits originais, dizemos que esse estado é **entrelaçado**

Estados de Bell são estados especiais em sistemas de 2 qubits que representam os exemplos mais simples de entrelaçamento quântico:

Estados de Bell são estados especiais em sistemas de 2 qubits que representam os exemplos mais simples de entrelaçamento quântico:

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

$$|\psi^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi^{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\psi^{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Estados de Bell são estados especiais em sistemas de 2 qubits que representam os exemplos mais simples de entrelaçamento quântico:

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

$$|\psi^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi^{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\psi^{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Vale ressaltar que os estados de Bell formam uma base do espaço de 2 qubits.

Estados de Bell são estados especiais em sistemas de 2 qubits que representam os exemplos mais simples de entrelaçamento quântico:

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

$$|\psi^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi^{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

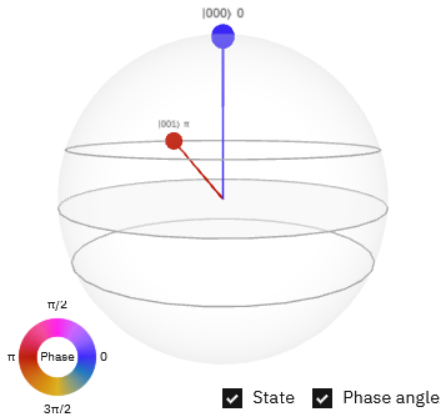
$$|\psi^{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Vale ressaltar que os estados de Bell formam uma base do espaço de 2 qubits.

Perceba como, nesses estados, uma medição no primeiro qubit imediatamente dá a informação de qual é o segundo qubit!

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Q-sphere



- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”
- 2 O produto interno entre dois estados: $\langle\varphi|U^*U|\psi\rangle = \langle\varphi|\psi\rangle$

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”
- 2 O produto interno entre dois estados: $\langle\varphi|U^*U|\psi\rangle = \langle\varphi|\psi\rangle$

Segue-se que todas essas transformações devem ser unitárias!

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”
- 2 O produto interno entre dois estados: $\langle\varphi|U^*U|\psi\rangle = \langle\varphi|\psi\rangle$

Segue-se que todas essas transformações devem ser unitárias!

$$U^* = U^{-1}$$

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”
- 2 O produto interno entre dois estados: $\langle\varphi|U^*U|\psi\rangle = \langle\varphi|\psi\rangle$

Segue-se que todas essas transformações devem ser unitárias!

$$U^* = U^{-1}$$

Cabe ressaltar que esta condição garante que os operadores sejam lineares:

Podemos definir operadores que, ao serem aplicados em um qubit, levam esse qubit de um estado a outro. Em notação bra-ket:

$$U|\psi_1\rangle = |\psi_2\rangle$$

Estas transformações devem preservar:

- 1 A regra de Born no novo estado, ou seja, a “norma”
- 2 O produto interno entre dois estados: $\langle\varphi|U^*U|\psi\rangle = \langle\varphi|\psi\rangle$

Segue-se que todas essas transformações devem ser unitárias!

$$U^* = U^{-1}$$

Cabe ressaltar que esta condição garante que os operadores sejam lineares:

$$U(a_1|\psi_1\rangle + \dots + a_n|\psi_n\rangle) = a_1U|\psi_1\rangle + \dots + a_nU|\psi_n\rangle$$

Um teorema essencial para a segurança de sistemas quânticos - e que será revisitado futuramente - é o teorema da não-clonagem.

Um teorema essencial para a segurança de sistemas quânticos - e que será revisitado futuramente - é o teorema da não-clonagem.

Devido às propriedades das transformações de estado, é impossível criar um operador capaz de clonar um estado quântico desconhecido $|a\rangle$:

Um teorema essencial para a segurança de sistemas quânticos - e que será revisitado futuramente - é o teorema da não-clonagem.

Devido às propriedades das transformações de estado, é impossível criar um operador capaz de clonar um estado quântico desconhecido $|a\rangle$:

$$\nexists U |U(|a\rangle|0\rangle) = |a\rangle|a\rangle$$

Um teorema essencial para a segurança de sistemas quânticos - e que será revisitado futuramente - é o teorema da não-clonagem.

Devido às propriedades das transformações de estado, é impossível criar um operador capaz de clonar um estado quântico desconhecido $|a\rangle$:

$$\nexists U |U(|a\rangle|0\rangle) = |a\rangle|a\rangle$$

Outra propriedade de sistemas quânticos é que toda transformação é reversível, uma vez que toda transformação deve ser unitária.

Transformações que operam sobre um número “pequeno” de qubits são chamadas **portas quânticas**. Essas portas representam os blocos fundamentais da computação quântica.

Transformações que operam sobre um número “pequeno” de qubits são chamadas **portas quânticas**. Essas portas representam os blocos fundamentais da computação quântica.

Portas podem ser classificadas de acordo com o número de qubits envolvidos. As mais comuns são:

- Portas 1-qubit: Pauli, Hadamard, Fase
- Portas 2-qubits: CNOT, swap, CZ
- Portas 3-qubits: Toffoli

As portas quânticas mais básicas são as portas X, Y e Z de Pauli. Cada porta representa uma rotação de π radianos na esfera de Bloch em relação ao eixo que dá o nome da porta.

As portas quânticas mais básicas são as portas X,Y e Z de Pauli.
Cada porta representa uma rotação de π radianos na esfera de Bloch em relação ao eixo que dá o nome da porta.

Definimos as portas como:

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = -|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Uma propriedade bastante importante da porta Pauli-X é que ela age como inversora dos estados $|0\rangle$ e $|1\rangle$ (o chamado “bit-flip”):

Uma propriedade bastante importante da porta Pauli-X é que ela age como inversora dos estados $|0\rangle$ e $|1\rangle$ (o chamado “bit-flip”):

$$\begin{cases} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{cases}$$

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Essa porta tem a propriedade de mapear os estados-base $\{|0\rangle, |1\rangle\}$ para os estados base $\{|+\rangle, |-\rangle\}$:

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Essa porta tem a propriedade de mapear os estados-base $\{|0\rangle, |1\rangle\}$ para os estados base $\{|+\rangle, |-\rangle\}$:

$$\begin{cases} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{cases}$$

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Essa porta tem a propriedade de mapear os estados-base $\{|0\rangle, |1\rangle\}$ para os estados base $\{|+\rangle, |-\rangle\}$:

$$\begin{cases} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{cases}$$

A porta Hadamard pode ser generalizada para múltiplos qubits. No caso especial onde partimos do estado $|0\rangle^{\otimes n}$

A porta Hadamard é provavelmente a porta mais importante da computação quântica. Ela é definida como:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Essa porta tem a propriedade de mapear os estados-base $\{|0\rangle, |1\rangle\}$ para os estados base $\{|+\rangle, |-\rangle\}$:

$$\begin{cases} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{cases}$$

A porta Hadamard pode ser generalizada para múltiplos qubits. No caso especial onde partimos do estado $|0\rangle^{\otimes n}$

$$H^{\otimes n}|0\rangle^{\otimes n} = (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}}(|0\dots 0\rangle + |0\dots 1\rangle + \dots + |1\dots 1\rangle) \triangleq |s_n\rangle$$

A Porta CNOT (“controlled not”) age em dois qubits. Ela inverte o segundo qubit se o primeiro qubit estiver no estado $|1\rangle$. Se o primeiro qubit estiver no estado $|0\rangle$, nada acontece:

A Porta CNOT (“controlled not”) age em dois qubits. Ela inverte o segundo qubit se o primeiro qubit estiver no estado $|1\rangle$. Se o primeiro qubit estiver no estado $|0\rangle$, nada acontece:

$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

A Porta CNOT (“controlled not”) age em dois qubits. Ela inverte o segundo qubit se o primeiro qubit estiver no estado $|1\rangle$. Se o primeiro qubit estiver no estado $|0\rangle$, nada acontece:

$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

$$\begin{cases} CNOT|00\rangle = |00\rangle \\ CNOT|01\rangle = |01\rangle \\ CNOT|10\rangle = |11\rangle \\ CNOT|11\rangle = |10\rangle \end{cases}$$

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Em circuitos quânticos:

Em circuitos quânticos:

- 1 Informação flui da esquerda para a direita

Em circuitos quânticos:

- 1 Informação flui da esquerda para a direita
- 2 Cada linha representa um único qubit

Em circuitos quânticos:

- 1 Informação flui da esquerda para a direita
- 2 Cada linha representa um único qubit
- 3 Portas são representadas por “quadrados”

Em circuitos quânticos:

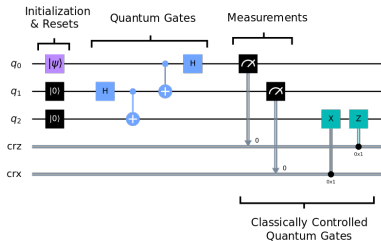
- 1 Informação flui da esquerda para a direita
- 2 Cada linha representa um único qubit
- 3 Portas são representadas por “quadrados”
- 4 Linhas duplas representam bits clássicos

Em circuitos quânticos:

- 1 Informação flui da esquerda para a direita
- 2 Cada linha representa um único qubit
- 3 Portas são representadas por “quadrados”
- 4 Linhas duplas representam bits clássicos
- 5 “Medições” convertem bits quânticos para clássicos. A conversão é direta: $M(|\psi\rangle) = |0\rangle \rightarrow 0$ e $M(|\psi\rangle) = |1\rangle \rightarrow 1$

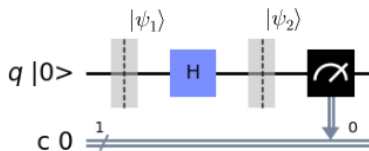
Em circuitos quânticos:

- 1 Informação flui da esquerda para a direita
- 2 Cada linha representa um único qubit
- 3 Portas são representadas por “quadrados”
- 4 Linhas duplas representam bits clássicos
- 5 “Medições” convertem bits quânticos para clássicos. A conversão é direta: $M(|\psi\rangle) = |0\rangle \rightarrow 0$ e $M(|\psi\rangle) = |1\rangle \rightarrow 1$

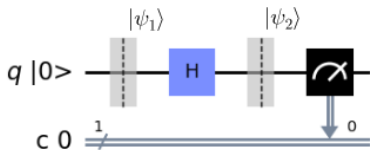


Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Considere o circuito simples abaixo:

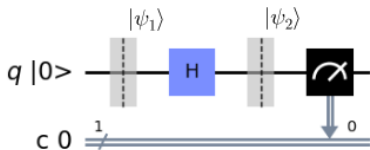


Considere o circuito simples abaixo:



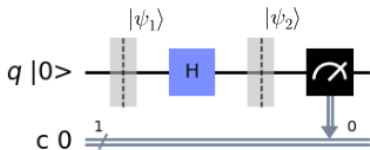
- 1 Começamos com um único qubit, que é inicializado no estado $|\psi_1\rangle = |0\rangle$

Considere o circuito simples abaixo:

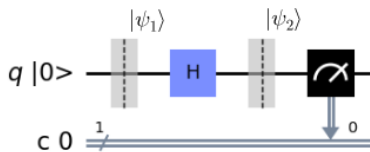


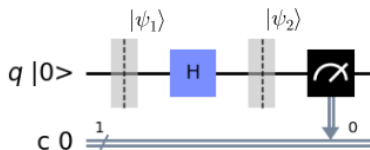
- 1 Começamos com um único qubit, que é inicializado no estado $|\psi_1\rangle = |0\rangle$
- 2 O qubit passa por uma porta Hadamard, alterando seu estado: $|\psi_2\rangle = H|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Considere o circuito simples abaixo:

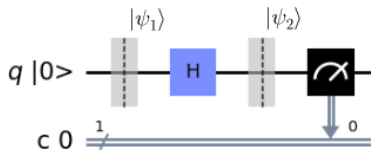


- 1 Começamos com um único qubit, que é inicializado no estado $|\psi_1\rangle = |0\rangle$
- 2 O qubit passa por uma porta Hadamard, alterando seu estado: $|\psi_2\rangle = H|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- 3 Fazemos uma medida do qubit para o bit clássico. Segundo a regra de Born, temos 50% de chance de medir o estado $|0\rangle \rightarrow 0$ e 50% de chance de medir o estado $|1\rangle \rightarrow 1$.

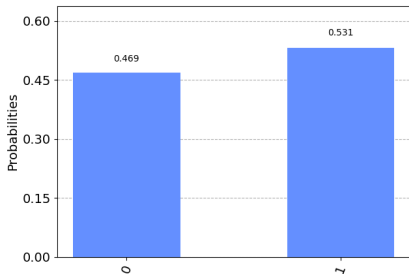




Testando o circuito 1024 vezes, obtemos um resultado condizente com o previsto:



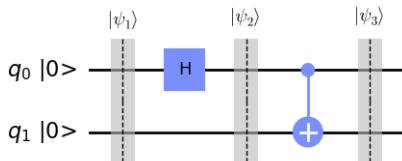
Testando o circuito 1024 vezes, obtemos um resultado condizente com o previsto:



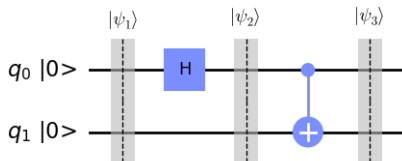
- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:

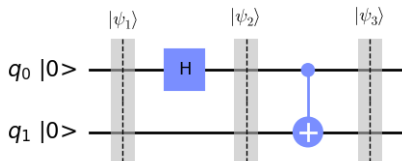


Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:



1 $|\psi_1\rangle = |0\rangle_{q_0} \otimes |0\rangle_{q_1}$

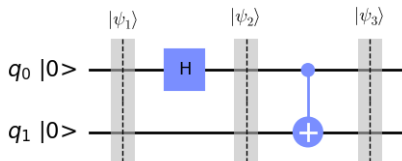
Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:



- 1 $|\psi_1\rangle = |0\rangle_{q_0} \otimes |0\rangle_{q_1}$

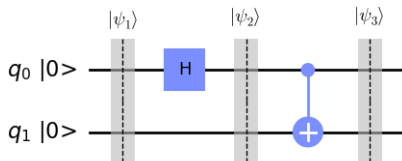
- 2 $|\psi_2\rangle = H|0\rangle_{q_0} \otimes |0\rangle_{q_1} = \frac{1}{\sqrt{2}}(|0\rangle_{q_0} \otimes |0\rangle_{q_1} + |1\rangle_{q_0} \otimes |0\rangle_{q_1})$

Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:



- 1 $|\psi_1\rangle = |0\rangle_{q_0} \otimes |0\rangle_{q_1}$
- 2 $|\psi_2\rangle = H|0\rangle_{q_0} \otimes |0\rangle_{q_1} = \frac{1}{\sqrt{2}}(|0\rangle_{q_0} \otimes |0\rangle_{q_1} + |1\rangle_{q_0} \otimes |0\rangle_{q_1})$
- 3 $|\psi_3\rangle = CNOT|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{q_0} \otimes |0\rangle_{q_1} + |1\rangle_{q_0} \otimes |1\rangle_{q_1})$

Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:



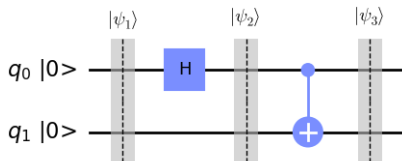
$$1 \quad |\psi_1\rangle = |0\rangle_{q0} \otimes |0\rangle_{q1}$$

$$2 \quad |\psi_2\rangle = H|0\rangle_{q0} \otimes |0\rangle_{q1} = \frac{1}{\sqrt{2}}(|0\rangle_{q0} \otimes |0\rangle_{q1} + |1\rangle_{q0} \otimes |0\rangle_{q1})$$

$$3 \quad |\psi_3\rangle = CNOT|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{q0} \otimes |0\rangle_{q1} + |1\rangle_{q0} \otimes |1\rangle_{q1})$$

$$|\psi_3\rangle = |\psi^{00}\rangle$$

Com o circuito abaixo, podemos construir o estado entrelaçado $|\psi^{00}\rangle$:



$$1 \quad |\psi_1\rangle = |0\rangle_{q0} \otimes |0\rangle_{q1}$$

$$2 \quad |\psi_2\rangle = H|0\rangle_{q0} \otimes |0\rangle_{q1} = \frac{1}{\sqrt{2}}(|0\rangle_{q0} \otimes |0\rangle_{q1} + |1\rangle_{q0} \otimes |0\rangle_{q1})$$

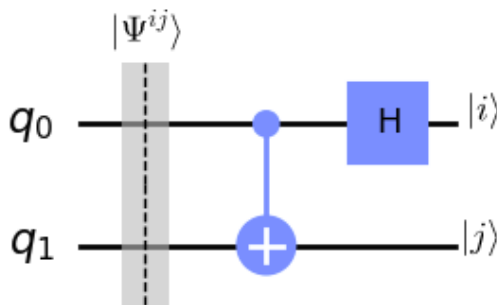
$$3 \quad |\psi_3\rangle = CNOT|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{q0} \otimes |0\rangle_{q1} + |1\rangle_{q0} \otimes |1\rangle_{q1})$$

$$|\psi_3\rangle = |\psi^{00}\rangle$$

Para obter outros estados, basta aplicar o mesmo circuito, mas mudando os valores iniciais em $|\psi_1\rangle$ aplicando portas X :

$$|\Psi^{ij}\rangle \rightarrow |\psi_1\rangle = |i\rangle_{q0} \otimes |j\rangle_{q1}$$

Temos agora o problema inverso: dado um estado de Bell $|\Psi^{ij}\rangle$, como medir i e j ? Podemos realizar o circuito inverso ao anterior! Como as matrizes H e $CNOT$ são reais, elas são suas próprias inversas:



- 1 Motivação
- 2 Sistemas de Um Qubit
 - Formalismo
 - Representação
- 3 Sistemas de Múltiplos Qubits
 - Formalismo
 - Representação
- 4 Operações Computacionais
 - Transformações Quânticas
 - Circuitos Quânticos
- 5 Exemplos Ilustrativos
 - Estados Entrelaçados
 - Protocolo de Teletransporte

Suponha que temos duas partes comunicantes, Alice e Bob.

Suponha que temos duas partes comunicantes, Alice e Bob.

Alice tem um certo estado quântico $|\phi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$ que ela deseja transmitir a Bob, mas entre os dois só existe um canal para bits clássicos.

Suponha que temos duas partes comunicantes, Alice e Bob.

Alice tem um certo estado quântico $|\phi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$ que ela deseja transmitir a Bob, mas entre os dois só existe um canal para bits clássicos.

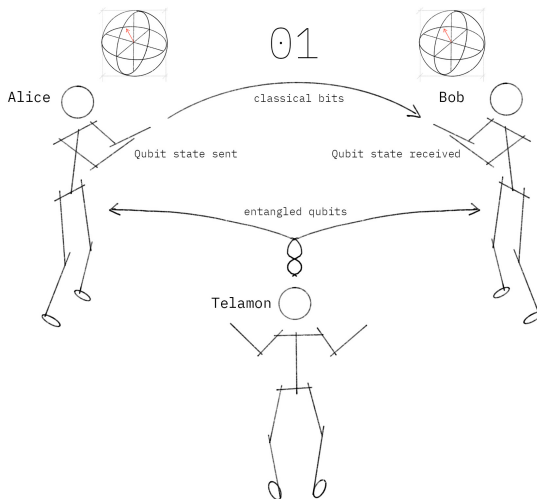
Foi previamente distribuído um estado entrelaçado $|\psi^{00}\rangle$ entre os dois.

Suponha que temos duas partes comunicantes, Alice e Bob.

Alice tem um certo estado quântico $|\phi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$ que ela deseja transmitir a Bob, mas entre os dois só existe um canal para bits clássicos.

Foi previamente distribuído um estado entrelaçado $|\psi^{00}\rangle$ entre os dois.

Como resolver esse problema?



Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

$$|\psi\rangle_{sab} = |\phi\rangle_s \otimes |\Psi^{00}\rangle_{ab} = (\alpha|0\rangle_s + \beta|1\rangle_s) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

$$|\psi\rangle_{sab} = |\phi\rangle_s \otimes |\Psi^{00}\rangle_{ab} = (\alpha|0\rangle_s + \beta|1\rangle_s) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

Reagrupando:

Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

$$|\psi\rangle_{sab} = |\phi\rangle_s \otimes |\Psi^{00}\rangle_{ab} = (\alpha|0\rangle_s + \beta|1\rangle_s) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

Reagrupando:

$$|\psi\rangle_{sab} = \frac{1}{\sqrt{2}}(\alpha|000\rangle_{sab} + \alpha|011\rangle_{sab} + \beta|100\rangle_{sab} + \beta|111\rangle_{sab})$$

Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

$$|\psi\rangle_{sab} = |\phi\rangle_s \otimes |\Psi^{00}\rangle_{ab} = (\alpha|0\rangle_s + \beta|1\rangle_s) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

Reagrupando:

$$|\psi\rangle_{sab} = \frac{1}{\sqrt{2}}(\alpha|000\rangle_{sab} + \alpha|011\rangle_{sab} + \beta|100\rangle_{sab} + \beta|111\rangle_{sab})$$

Podemos manipular algebricamente o estado, obtendo:

Suponha que Alice tem um qubit do estado entrelaçado enquanto Bob tem o outro qubit. Podemos escrever o estado total do sistema:

$$|\psi\rangle_{sab} = |\phi\rangle_s \otimes |\Psi^{00}\rangle_{ab} = (\alpha|0\rangle_s + \beta|1\rangle_s) \otimes \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

Reagrupando:

$$|\psi\rangle_{sab} = \frac{1}{\sqrt{2}}(\alpha|000\rangle_{sab} + \alpha|011\rangle_{sab} + \beta|100\rangle_{sab} + \beta|111\rangle_{sab})$$

Podemos manipular algebricamente o estado, obtendo:

$$\begin{aligned} |\psi\rangle_{sab} = \frac{1}{2\sqrt{2}} & [(|00\rangle_{sa} + |11\rangle_{sa}) \otimes (\alpha|0\rangle_b + \beta|1\rangle_b) \\ & + (|01\rangle_{sa} + |10\rangle_{sa}) \otimes (\alpha|1\rangle_b + \beta|0\rangle_b) \\ & + (|00\rangle_{sa} - |11\rangle_{sa}) \otimes (\alpha|0\rangle_b - \beta|1\rangle_b) \\ & + (|01\rangle_{sa} - |10\rangle_{sa}) \otimes (\alpha|1\rangle_b - \beta|0\rangle_b)] \end{aligned}$$

Manipulando o resultado anterior:

Manipulando o resultado anterior:

$$\begin{aligned} |\psi\rangle_{sab} = & \frac{1}{2} [|\psi^{00}\rangle_{sa} \otimes |\phi\rangle_b \\ & + |\psi^{01}\rangle_{sa} \otimes X|\phi\rangle_b \\ & + |\psi^{10}\rangle_{sa} \otimes Z|\phi\rangle_b \\ & + |\psi^{11}\rangle_{sa} \otimes XZ|\phi\rangle_b] \end{aligned}$$

Manipulando o resultado anterior:

$$\begin{aligned} |\psi\rangle_{sab} = & \frac{1}{2} [|\psi^{00}\rangle_{sa} \otimes |\phi\rangle_b \\ & + |\psi^{01}\rangle_{sa} \otimes X|\phi\rangle_b \\ & + |\psi^{10}\rangle_{sa} \otimes Z|\phi\rangle_b \\ & + |\psi^{11}\rangle_{sa} \otimes XZ|\phi\rangle_b] \end{aligned}$$

Chegamos a um resultado inacreditável: realizando uma medida de Bell nos qubits sa e transmitindo o resultado com bits clássicos, Bob pode receber o estado $|\phi\rangle$

O circuito abaixo implementa o protocolo de teletransporte descrito

