Sistemas com múltiplos qubits

Adenilton José da Silva

3 de setembro de 2020

Introdução

- Existe uma enorme diferença entre a dimensão de sistemas clássicos e sistemas quânticos.

Introdução

- Existe uma enorme diferença entre a dimensão de sistemas clássicos e sistemas quânticos.
- Utilizamos o produto tensorial para combinar espaços vetorais em espaços vetoriais maiores.

Introdução

- Existe uma enorme diferença entre a dimensão de sistemas clássicos e sistemas quânticos.
- Utilizamos o produto tensorial para combinar espaços vetorais em espaços vetoriais maiores.
- O estado de alguns sistemas quânticos não podem ser descritos pela descrição do estado de cada um de seus componentes de forma separada.

Introdução

- Existe uma enorme diferença entre a dimensão de sistemas clássicos e sistemas quânticos.
- Utilizamos o produto tensorial para combinar espaços vetorais em espaços vetoriais maiores.
- O estado de alguns sistemas quânticos não podem ser descritos pela descrição do estado de cada um de seus componentes de forma separada.
- O emaranhamento é uma característica única de sistemas quânticos.

Seção 1

Produto tensorial

Produto tensorial

Definição

- O **produto tensorial** $V \otimes W$ de dois espaços vetoriais V e W com bases $A = \{|\alpha_1\rangle, \cdots, |\alpha_n\rangle\}$ e $B = \{|\beta_1\rangle, \cdots, |\beta_m\rangle\}$ é um espaço vetorial cuja base possui nm elementos com a forma $|\alpha_i\rangle \otimes |\beta_j\rangle$, onde $\otimes$ satisfaz:
  i. $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
  ii. $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$
  iii. $(a|v\rangle) \otimes |w\rangle = |v\rangle \otimes (a|w\rangle) = a(|v\rangle \otimes |w\rangle)$

Produto tensorial

Exemplo

- Considere a base $\{|0\rangle, |1\rangle\}$ de $\mathbb{V} = \mathbb{C}^2$.
- $\mathbb{V} \otimes \mathbb{V}$ é o espaço vetorial sobre o corpo dos complexos gerado pela base

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$$

- Elementos do espaço vetorial $\mathbb{C}^2 \otimes \mathbb{C}^2$ podem ser escritos como

$$a_{00}|0\rangle \otimes |0\rangle + a_{01}|0\rangle \otimes |1\rangle + a_{10}|1\rangle \otimes |0\rangle + a_{11}|1\rangle \otimes |1\rangle$$

Produto tensorial

Exemplo

- Considere o espaço vetorial $\mathbb{V} = \mathbb{C}^2$ e a base $\{|0\rangle, |1\rangle\}$.
- Se $|v\rangle = a_0 |0\rangle + a_1 |1\rangle$ e $|w\rangle = b_0 |0\rangle + b_1 |1\rangle$.
- $|v\rangle \otimes |w\rangle = (a_0 |0\rangle + a_1 |1\rangle) \otimes (b_0 |0\rangle + b_1 |1\rangle) =$

$$a_0 b_0 (|0\rangle \otimes |0\rangle) + a_0 b_1 (|0\rangle \otimes |1\rangle) + a_1 b_0 (|1\rangle \otimes |0\rangle) + a_1 b_1 (|1\rangle \otimes |1\rangle)$$

Produto interno

- Se $\mathbb{V}$ e $\mathbb{W}$ possuem produto interno, então o produto interno dos vetores $|v_1\rangle \otimes |w_1\rangle$ e $|v_2\rangle \otimes |w_2\rangle$ em $\mathbb{V} \otimes \mathbb{W}$ é dado por

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle \cdot \langle w_2|w_1\rangle$$

Produto interno

- Se $\mathbb{V}$ e $\mathbb{W}$ possuem produto interno, então o produto interno dos vetores $|v_1\rangle \otimes |w_1\rangle$ e $|v_2\rangle \otimes |w_2\rangle$ em $\mathbb{V} \otimes \mathbb{W}$ é dado por

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle \cdot \langle w_2|w_1\rangle$$

- O produto tensorial de dois vetores unitários resulta em um vetor unitário

Produto interno

- Se $\mathbb{V}$ e $\mathbb{W}$ possuem produto interno, então o produto interno dos vetores $|v_1\rangle \otimes |w_1\rangle$ e $|v_2\rangle \otimes |w_2\rangle$ em $\mathbb{V} \otimes \mathbb{W}$ é dado por

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle \cdot \langle w_2|w_1\rangle$$

- O produto tensorial de dois vetores unitários resulta em um vetor unitário
- Sejam $\{|\alpha_i\rangle\}$ uma base ortonormal de $\mathbb{V}$ e $\{|\beta_i\rangle\}$ uma base ortonormal de $\mathbb{W}$, então $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ é uma base ortonormal de $\mathbb{V} \otimes \mathbb{W}$.

Emaranhamento

- Existem elementos em $\mathbb{V} \otimes \mathbb{W}$ que não podem ser escritos com $|v\rangle \otimes |w\rangle$.
  - Dizemos que estes estados estão **emaranhados**.

Emaranhamento

Exemplo

- Verifique que o estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ está emaranhado.

Seção 2

Sistemas com múltiplos qubits

Múltiplos qubits

- Seja $\mathbb{V}_i$ um espaço vetorial com base $\{|0\rangle_i, |1\rangle_i\}$, $i = 0, \cdots, n-1$.
- Um sistema quântico com n-qubits é descrito por um vetor unitário no espaço vetorial $\mathbb{V}_{n-1} \otimes \cdots \otimes \mathbb{V}_0$ que possui a base

$$\left\{ \begin{array}{c} |0\rangle_{i-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0, \\ |0\rangle_{i-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0, \\ |0\rangle_{i-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0, \\ \vdots \\ |1\rangle_{i-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0 \end{array} \right\}$$

Múltiplos qubits

- Seja $\mathbb{V}_i$ um espaço vetorial com base $\{|0\rangle_i, |1\rangle_i\}$, $i = 0, \cdots, n-1$.
- Um sistema quântico com n-qubits é descrito por um vetor unitário no espaço vetorial $\mathbb{V}^{\otimes n} = \mathbb{V} \otimes \cdots \otimes \mathbb{V}$ que possui a base

$$\left\{ \begin{array}{c} |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle, \\ |0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle, \\ |0\rangle \otimes \cdots \otimes |1\rangle \otimes |0\rangle, \\ \vdots \\ |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle \end{array} \right\}$$

Múltiplos qubits

- Seja $\mathbb{V}_i$ um espaço vetorial com base $\{|0\rangle_i, |1\rangle_i\}$, $i = 0, \cdots, n-1$.
- Um sistema quântico com n-qubits é descrito por um vetor unitário no espaço vetorial $\mathbb{V}^{\otimes n} = \mathbb{V} \otimes \cdots \otimes \mathbb{V}$ que possui a base

$$\left\{ \begin{array}{c} |0\rangle \cdots |0\rangle |0\rangle, \\ |0\rangle \cdots |0\rangle |1\rangle, \\ |0\rangle \cdots |1\rangle |0\rangle, \\ \vdots \\ |1\rangle \cdots |1\rangle |1\rangle \end{array} \right\}$$

Múltiplos qubits

- Seja $\mathbb{V}_i$ um espaço vetorial com base $\{|0\rangle_i, |1\rangle_i\}$, $i = 0, \cdots, n-1$.
- Um sistema quântico com n-qubits é descrito por um vetor unitário no espaço vetorial $\mathbb{V}^{\otimes n} = \mathbb{V} \otimes \cdots \otimes \mathbb{V}$ que possui a base

$$\left\{ \begin{array}{c} |0\cdots00\rangle, \\ |0\cdots01\rangle, \\ |0\cdots10\rangle, \\ \vdots \\ |1\cdots11\rangle \end{array} \right\}$$

Múltiplos qubits

- Seja $\mathbb{V}_i$ um espaço vetorial com base $\{|0\rangle_i, |1\rangle_i\}$, $i = 0, \cdots, n-1$.
- Um sistema quântico com n-qubits é descrito por um vetor unitário no espaço vetorial $\mathbb{V}^{\otimes n} = \mathbb{V} \otimes \cdots \otimes \mathbb{V}$ que possui a base

$$\left\{ \begin{array}{c} |0\rangle, \\ |1\rangle, \\ |2\rangle, \\ \vdots \\ |2^n - 1\rangle \end{array} \right\}$$

Múltiplos qubits

Exemplos

- $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$

Múltiplos qubits

Exemplos

- $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$
- Utilizando a base $\{|000\rangle, |001\rangle, \cdots, |111\rangle\}$ este estado tem representação matricial

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

O espaço dos múltiplos qubits

- O espaço de um sistema com múltiplos qubits é diferente do espaço vetorial em que ele é representado.
- Diferentes vetores podem representar o mesmo qubit.

Fase global

- Vetores diferem apenas por uma fase global representam o mesmo estado quântico.

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \sim \frac{e^{i\theta}}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- $|00\rangle \sim e^{i\theta}|00\rangle$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \not\sim \frac{e^{i\theta}|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \sim \frac{e^{i\theta}|00\rangle + e^{i\theta}|11\rangle}{\sqrt{2}}$$

Representação única

- Seja $|v\rangle = a_0 |0\rangle + \cdots + a_{2^n-1} |2^n - 1\rangle$ um estado quântico com n qubits.
- Se escrevermos todos os estados quânticos com fazendo o primeiro a_i não nulo um número real positivo, então a representação dos qubits será única.

Emaranhamento

- Um array com qubits $[|v_0\rangle, |v_1\rangle, \cdots, |v_n\rangle]$ tem um crescimento linear em relação ao número de qubits.

Emaranhamento

- Um array com qubits $[|v_0\rangle, |v_1\rangle, \cdots, |v_n\rangle]$ tem um crescimento linear em relação ao número de qubits.
- O produto tensorial $|v_0\rangle \otimes |v_1\rangle \otimes \cdots \otimes |v_n\rangle$ tem um crescimento exponencial em relação ao número de qubits.

Emaranhamento

- Um array com qubits $[|v_0\rangle, |v_1\rangle, \cdots, |v_n\rangle]$ tem um crescimento linear em relação ao número de qubits.
- O produto tensorial $|v_0\rangle \otimes |v_1\rangle \otimes \cdots \otimes |v_n\rangle$ tem um crescimento exponencial em relação ao número de qubits.
- A maior parte dos estados com n qubits não pode ser descrita pelo estado de n qubits de forma separada.

Emaranhamento

Exemplos

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Seção 3

Medição

Medição

- Medição do primeiro qubit utilizando a base $\{|0\rangle, |1\rangle\}$
  $a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$
- $|0\rangle$ com probabilidade $|a_0|^2 + |a_1|^2$, estado após medição

$$|0\rangle \left(\frac{a_0 |0\rangle + a_1 |1\rangle}{\sqrt{|a_0|^2 + |a_1|^2}} \right) = \left(\frac{a_0 |00\rangle + a_1 |01\rangle}{\sqrt{|a_0|^2 + |a_1|^2}} \right)$$

Medição

- Medição do primeiro qubit utilizando a base $\{|0\rangle, |1\rangle\}$
  $a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$
- $|0\rangle$ com probabilidade $|a_0|^2 + |a_1|^2$, estado após medição

$$|0\rangle \left(\frac{a_0 |0\rangle + a_1 |1\rangle}{\sqrt{|a_0|^2 + |a_1|^2}} \right) = \left(\frac{a_0 |00\rangle + a_1 |01\rangle}{\sqrt{|a_0|^2 + |a_1|^2}} \right)$$

- $|1\rangle$ com probabilidade $|a_2|^2 + |a_3|^2$, estado após medição

$$|1\rangle \left(\frac{a_2 |0\rangle + a_3 |1\rangle}{\sqrt{|a_2|^2 + |a_3|^2}} \right) = \left(\frac{a_2 |10\rangle + a_3 |11\rangle}{\sqrt{|a_2|^2 + |a_3|^2}} \right)$$

Medição

- Medição do primeiro qubit utilizando a base $\{|+\rangle, |-\rangle\}$
  $a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$
- Reescreva o estado utilizando a base $\{|+\rangle, |-\rangle\}$ para determinar o resultado da medição.

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|0\rangle, |1\rangle\}$.

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|0\rangle, |1\rangle\}$.
  - $|0\rangle$ com probabilidade 50%, estado resultante $|00\rangle$.
  - $|1\rangle$ com probabilidade 50%, estado resultante $|11\rangle$.

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|0\rangle, |1\rangle\}$.
  - $|0\rangle$ com probabilidade 50%, estado resultante $|00\rangle$.
  - $|1\rangle$ com probabilidade 50%, estado resultante $|11\rangle$.
- Qual o resultado da medição do segundo qubit?

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|+\rangle, |-\rangle\}$.

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|+\rangle, |-\rangle\}$.
  - $|+\rangle$ com probabilidade 50%, estado resultante $|+\rangle|+\rangle$.
  - $|-\rangle$ com probabilidade 50%, estado resultante $|-\rangle|-\rangle$.

Medição

Exemplo

- Medição do primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ utilizando a base $\{|+\rangle, |-\rangle\}$.
  - $|+\rangle$ com probabilidade 50%, estado resultante $|+\rangle|+\rangle$.
  - $|-\rangle$ com probabilidade 50%, estado resultante $|-\rangle|-\rangle$.
- Qual o resultado da medição do segundo qubit?

Seção 4

Distribuição de chaves utilizando estados emaranhados

Distribuição de chaves utilizando estados emaranhados

- Compartilhar um estado $|00\rangle + |11\rangle$
- Alice faz a medição do primeiro qubit escolhendo aleatoriamente uma das bases $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$
- Bob faz a medição do segundo qubit escolhendo aleatoriamente uma das bases $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$
- Se as bases não coincidirem o bit resultante é descartado. Se as bases coincidirem o bit resultante irá compor a chave.