Quantum Phase Estimation (QPE)

. Esse algoritmo é uma das subrotinas mais utilizadas em computação quântica.

. Esse algoritmo algumas vezes é estimador de autovalor.

DON'T FORGET

ÁLGEBRA LINEAR

Dada uma matriz M e um vetor $|v\rangle$ dizemos que $|v\rangle$ é um autovetor de M se $M|v\rangle = \lambda|v\rangle$ onde λ é o autovalor associado ao autovetor $|v\rangle$

1) Seja $|\psi\rangle$ um estado quântico.

$$|\psi\rangle = \sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1} w_k\,|k_1 k_2 \ldots k_n\rangle \quad \text{onde} \quad \sum_k |w_k|^2 = 1$$

. Esse estado pode ser genérico e não precisamos ter qualquer qualquer informação

2) Seja U um operador e $|\psi\rangle$ um autoestado de U

$$\underbrace{U}_{\text{Operador de rotação}}|\psi\rangle = \underbrace{e^{2\pi i\theta}}_{\text{autovalor}}\,\underbrace{|\psi\rangle}_{\text{autovetor}}$$

Objetivo do algoritmo

- Dado um operador unitário U
- Algoritmo estima θ → phase

$$\underbrace{U}_{\substack{\text{operador}\\\text{(matriz)}}}|\psi\rangle = \underbrace{e^{2\pi i\theta}}_{\substack{\text{autovalor}\\\text{associado}\\\text{a } |\psi\rangle}}|\psi\rangle$$

→ autovetor de U

Extra:

O que significa U ser uma matriz unitária?

$$UU^{-1} = \mathbb{1}$$

Ex:

- $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \xrightarrow[\text{por coluna}]{\text{trocar linha}} H^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\boxed{H = H^{-1}}$

- matriz unitária implica na soma do módulo quadrado dos autovalores deve somar 1.

Ex: $H \xrightarrow[\text{autovalores}]{\text{tem como}} \lambda_1$ e λ_2 $\quad \sum_{i=1}^{2} |\lambda_i|^2 = 1$

$|\lambda_i|^2$ → probabilidade de obter o autovetor $|\psi_i\rangle$

vínculo probabilidade

Abaixo vamos mostrar a "cara" do circuito QPE

Step 0: $|\psi\rangle$ → Estado que você quer estimar a fase

Step 1: n qubits (chamados de counting qubits) que serão utilizados para estimar a phase.

$$|\psi_0\rangle = |0\rangle^{\otimes n}|\psi\rangle$$

Step 2: Superposição nos "counting qubits"

$$|\psi_1\rangle = \underbrace{H^{\otimes n}|0\rangle^{\otimes n}}\otimes\underbrace{\mathbb{I}|\psi\rangle}$$ → aplicando Hadamard em $|0\rangle^{\otimes n}$ e identidade ($\mathbb{I}$) em $|\psi\rangle$

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

$$|\psi_1\rangle = \underbrace{\frac{1}{\sqrt{2^{n/2}}}(|0\rangle + |1\rangle)^{\otimes n}}_{\text{Superposição}} \otimes |\psi\rangle$$

Step 3: Aplicar U em $|\psi\rangle$. Vamos analisar apenas U agindo em $|\psi\rangle$ e depois entender controled U gate.

1. Vamos aplicar U^{2^j} em $|\psi\rangle$

(1) $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$

(2) $U^2|\psi\rangle = e^{2\pi i\theta} U|\psi\rangle = e^{2\pi i\theta} e^{2\pi i\theta}|\psi\rangle = e^{2.(2\pi i\theta)}|\psi\rangle$

(3) $U^3|\psi\rangle = U\underbrace{U^2|\psi\rangle} = e^{2.(2\pi i\theta)}\underbrace{U|\psi\rangle} = e^{3(2\pi i\theta)}|\psi\rangle$

(4) $U^N|\psi\rangle = \underbrace{U\cdots U^3}_{N \text{ vezes}}|\psi\rangle = e^{N(2\pi i\theta)}|\psi\rangle$

- Quando $N = 2^j$ e $j = n-1$, onde n = número de qubits in the counting register, nós temos

$$\boxed{U^{2^j}|\psi\rangle = e^{2^j(2\pi i\theta)}|\psi\rangle}$$

- Agora que já sabemos como U^{2^j} atua em $|\psi\rangle$ vamos entender a "versão controlada" do gate.

* Nosso estado completo é:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)^{\otimes n}\otimes|\psi\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\Big[\overbrace{(|0\rangle+|1\rangle)}^{|q_0\rangle}\otimes\overbrace{(|0\rangle+|1\rangle)}^{|q_1\rangle}\otimes\cdots\otimes\overbrace{(|0\rangle+|1\rangle)}^{q_{n-1}}\Big]\otimes|\psi\rangle$$

* Aplicando cU^N em $|\psi_1\rangle$ temos (se o qubit do counting é $|1\rangle$ aplica U em $|\psi\rangle$ → ordenamento do qubit $n-k$

$$|\psi_2\rangle = cU^N|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\Big[\underbrace{cU^{2^{n-1}}(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle)}_{k=1}\otimes cU^{2^{n-2}}(|0\rangle|\psi\rangle+|1\rangle|\psi\rangle)\otimes\cdots$$
$$\cdots\otimes cU^{2^0}(|0\rangle|\psi\rangle+|1\rangle|\psi\rangle)\Big]$$

c ↓ condicionado ao qubit

$$= \frac{1}{\sqrt{2^n}}\Big[(|0\rangle + e^{2^{n-1}(2\pi i\theta)}|1\rangle)\otimes(|0\rangle + e^{2^{n-2}(2\pi i\theta)}|1\rangle)\otimes\cdots$$
$$\otimes(|0\rangle + e^{2^0(2\pi i\theta)}|1\rangle)\otimes|\psi\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{k=1}^{n} e^{2\pi i\theta k}|k\rangle\otimes|\psi\rangle$$

↳ inteira de uma seq. binária

$k = (0, 1, \ldots n)$ → representação Inteira da sequência binária

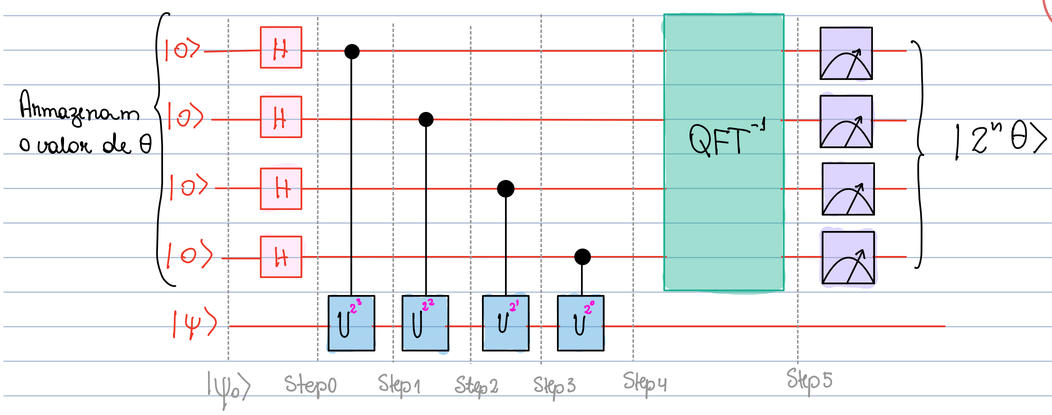
Ex: $|\underset{2^2}{1}\,\underset{2^1}{0}\,\underset{2^0}{1}\rangle \Rightarrow |5\rangle$

$2^2 \cdot 1 + 2^1 \cdot 0 + 2^0 \cdot 1 = 4 + 0 + 1 = 5$

Portanto $$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_k e^{2\pi i \theta k} |k\rangle \otimes |\psi\rangle$$

Exemplo com quatro qubits:

$n = 4$



Initial State

$$|\psi_0\rangle = \underbrace{|0_0\rangle}_{q_1} \otimes \underbrace{|0_1\rangle}_{q_2} \otimes \underbrace{|0_2\rangle}_{q_3} \otimes \underbrace{|0_3\rangle}_{q_4} \otimes |\psi\rangle = |0_0 0_1 0_2 0_3\rangle \otimes |\psi\rangle \qquad n = 4$$

Step 0: Aplicando Hadamard nos qubits de contagem

$$H^{\otimes}|0_0 0_1 0_2 0_3\rangle = \frac{1}{4}(|0_0\rangle + |1_0\rangle) \otimes (|0_1\rangle + |1_1\rangle) \otimes (|0_2\rangle + |1_2\rangle) \otimes (|0_3\rangle + |1_3\rangle)$$

O Estado fica:

$$|\psi_1\rangle = \frac{1}{4}(|0\rangle_0 + |1\rangle_0) \otimes (|0\rangle_1 + |1\rangle_1) \otimes (|0\rangle_2 + |1\rangle_2) \otimes (|0\rangle_3 + |1\rangle_3) \otimes |\psi\rangle$$

Step 1: Aplicando U em $|\psi\rangle$ se $|q_0\rangle = |1\rangle$ – controlled U

$\underline{\underline{q_0}} \longrightarrow \underline{\underline{U}}^{2^{n-1}}$

$$|\psi_2\rangle = cU^{\underline{\underline{2^3}}}|\psi_1\rangle = \frac{1}{4}(|0_0\rangle + cU^{2^3}\,\underline{\underline{|1\rangle}} \otimes |\psi\rangle) \otimes \cdots$$

$\hookrightarrow q_0$ como qubit controle

$$= \frac{1}{4}(|0_0\rangle + e^{(2\pi i \theta) 2^3}|1\rangle) \otimes |\psi\rangle \otimes \cdots$$

$$|\psi_2\rangle = \frac{1}{4}(|0_0\rangle + e^{(2\pi i \theta) 2^3}|1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |\psi\rangle$$

Step 2 : Aplicar cU $|q_1\rangle \longrightarrow |\psi\rangle$

↳ controle

$$|\psi_3\rangle = \frac{1}{4}\left(|0\rangle + e^{(2\pi i\theta)2^3}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^2}|1\rangle\right)\otimes\left(|0\rangle + |1\rangle\right)\otimes\left(|0\rangle + |1\rangle\right)\otimes|\psi\rangle$$

Step 3: Aplicar cU $\underset{|q_2\rangle}{c} \longrightarrow \underset{|\psi\rangle}{t}$

$$|\psi_4\rangle = \frac{1}{4}\left(|0\rangle + e^{(2\pi i\theta)2^3}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^2}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^1}|1\rangle\right)\otimes\left(|0\rangle + |1\rangle\right)\otimes|\psi\rangle$$

Step 4: Aplicar cU $|q_3\rangle \longrightarrow |\psi\rangle$

$$|\psi_5\rangle = \frac{1}{4}\left(|0\rangle + e^{(2\pi i\theta)2^3}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^2}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^1}|1\rangle\right)\otimes\left(|0\rangle + e^{(2\pi i\theta)2^0}|1\rangle\right)\otimes|\psi\rangle$$

Abrindo produto tensorial acima temos:

$$|\psi_5\rangle = \frac{1}{4}\Big[|0000\rangle + e^{(2\pi i\theta)1}|0001\rangle + e^{(2\pi i\theta)2}|0010\rangle + e^{3(2\pi i\theta)}|0011\rangle + e^{4(2\pi i\theta)}|0100\rangle$$
$$+ e^{5(2\pi i\theta)}|0101\rangle + e^{6(2\pi i\theta)}|0110\rangle + e^{7(2\pi i\theta)}|0111\rangle + e^{8(2\pi i\theta)}|1000\rangle$$
$$+ e^{9(2\pi i\theta)}|1001\rangle + e^{10(2\pi i\theta)}|1010\rangle + e^{11(2\pi i\theta)}|1011\rangle + e^{12(2\pi i\theta)}|1100\rangle$$
$$+ e^{13(2\pi i\theta)}|1101\rangle + e^{14(2\pi i\theta)}|1110\rangle + e^{15(2\pi i\theta)}|1111\rangle\Big]$$

padrão percebido ?

Se olharmos bem expoente que multiplica o termo $(2\pi i\theta)$ é a representação inteira da sequência binária que aparecem nos estados quânticos. Ou seja:

$|0001\rangle \longrightarrow 1$

$|0010\rangle \longrightarrow 2$

$|0011\rangle \longrightarrow 3$

⋮

De maneira geral: Dado o estado $|q_0\, q_1\, q_2\, q_3\rangle$

$\downarrow$ 2^3 2^2 2^1 2^0

número inteiro

$$K = q_0 2^3 + q_1 2^2 + q_2 2^1 + q_3 2^0$$

A expressão de $|\psi_5\rangle$ pode ser escrita como:

$$|\psi_5\rangle = \frac{1}{\sqrt{2^n}}\sum_{K=0}^{2^n-1} e^{2\pi i\theta K}|K\rangle$$

com $n = 4$

Step 5: Aplicar QFT^{-1} nos qubits de contagem:

1) Vamos relembrar o que o QFT faz.

$$|\tilde{x}\rangle = QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle$$ $|y$

$|y\rangle$ ↳ inteira

Obs: binário ⟶ inteiro

$$|y\rangle = |y_1 y_2 y_3 \cdots y_n\rangle \qquad \{y_1, y_2, \dots, y_n\} \in \{0,1\}$$

(int)

$$y = 2^{n-1} y_1 + 2^{n-2} y_2 + 2^{n-3} y_3 + \cdots 2^{n-n} y_n$$

$$y = \sum_{k=1}^{n} 2^{n-k} y_k$$

$$\frac{y}{2^n} = \sum_{k=1}^{n} \frac{y_k}{2^k}$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_1, y_2, \dots = 0} e^{2\pi i x \sum_{k=1}^{n} y_k/2^k} |y_1 y_2 \dots y_n\rangle$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_1} \sum_{y_2} \cdots \sum_{y_n} e^{2\pi i x \left(y_1/2^1 + y_2/2^2 + \cdots y_n/2^n \right)} |y_1 y_2 \dots y_n\rangle$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_1} \sum_{y_2} \cdots \sum_{y_n} e^{\frac{2\pi i x y_1}{2^1}} \cdot e^{2\pi i x y_2/2^2} \cdots e^{2\pi i x y_n/2^n} |y_1 y_2 \cdots y_n\rangle$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_1=0}^{1} e^{2\pi i x y_1/2^1} |y_1\rangle \otimes \sum_{y_2=0}^{1} e^{2\pi i x y_2/2^2} |y_2\rangle \otimes \cdots \otimes \sum_{y_n=0}^{1} e^{2\pi i x y_n/2^n} |y_n\rangle$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \underbrace{\left(|0\rangle + e^{2\pi i x/2^1} |1\rangle\right)}_{k = \text{ ordenamento do qubit}} \otimes \left(|0\rangle + e^{2\pi i x/2^2} |1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i x/2^n} |1\rangle\right)$$

int

inteiro

obs: $X = |x_1 x_2 x_3 \dots x_n\rangle$

Retomando a Expressão:

$$|\psi_5\rangle = \frac{1}{4}\left(|0\rangle + e^{(2\pi i \theta) 2^3} |1\rangle\right) \otimes \left(|0\rangle + e^{(2\pi i \theta) 2^2} |1\rangle\right) \otimes \left(|0\rangle + e^{(2\pi i \theta) 2^1} |1\rangle\right) \otimes \left(|0\rangle + e^{(2\pi i \theta) 2^0} |1\rangle\right) \otimes |\psi\rangle$$

$2^{4-1}\theta$ → $2^{n-1}\theta$; $2^{4-2}\theta$ → $2^{n-2}\theta$; $2^{n-3}\theta$; $2^{n-n}\theta$

* com $n=4$

$$e^{\left(2\pi i\, 2^{n-k} \theta\right)} = e^{\frac{2\pi i (2^n \theta)}{2^k}} \quad |x = 2^n \theta\rangle$$

$\curvearrowright n=$

\# Podemos reescrever a expressão acima da seguinte forma:

$$|\psi_5\rangle = \frac{1}{4}\left(|0\rangle + e^{\frac{2\pi i (2^n\theta)}{2}}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{2\pi i (2^n\theta)}{2^2}}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{2\pi i (2^n\theta)}{2^3}}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{2\pi i (2^n\theta)}{2^n}}|1\rangle\right)$$

Comparando $|\psi_5\rangle$ com a expressão do $QFT|x\rangle$ podemos associar x como sendo $2^n\theta$, ou seja

$$|x\rangle = |2^n\theta\rangle$$

$$|\psi_5\rangle \equiv QFT|2^n\theta\rangle$$

$$QFT^{-1}|\psi_5\rangle = \underbrace{QFT^{-1}QFT}_{\mathbb{I}}|2^n\theta\rangle$$

$$QFT^{-1}|\psi_5\rangle = |2^n\theta\rangle$$

* Se aplicarmos $QFT^{-1}|\tilde{x}\rangle$ obteremos o estado $|x\rangle$

O estado $|\psi_5\rangle$ é a transforma de Fourier do estado $|2^n\theta\rangle$. Para obter $|2^n\theta\rangle$ teremos que aplicar QFT^{-1}.

$$QFT^{-1}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{-\frac{2\pi i x y}{2^n}}|y\rangle$$

$$QFT^{-1}|\psi_5\rangle = |2^n\theta\rangle$$

$$\theta = \frac{int(|\text{binário}\rangle)}{2^n}$$

(não deu tempo de fazer continhas)

abrir posteriormente