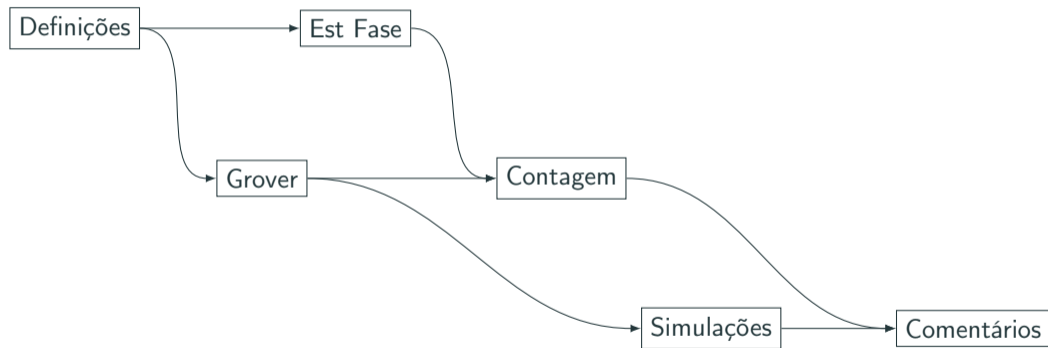


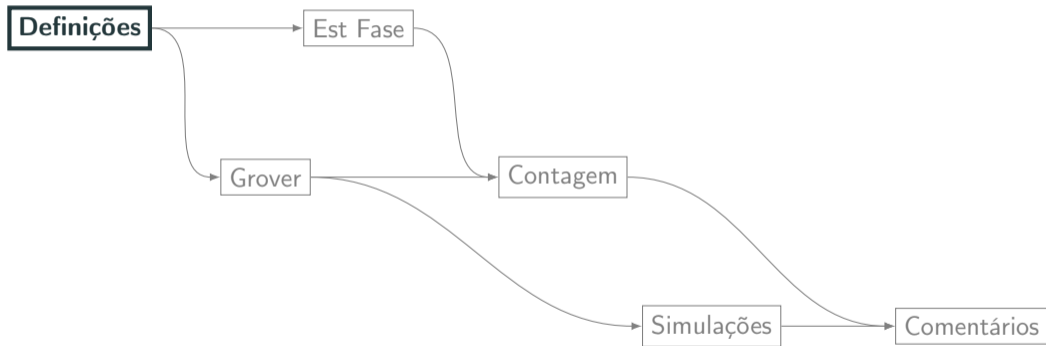
Computação Quântica e suas Bases Teóricas

Gustavo Alves Bezerra

13 de dezembro de 2024

gustavowl.github.io





- Vetores unitários $|\psi\rangle \in \mathcal{H}^N$, $N = 2^n$;
 $|\psi\rangle = a_0 |0\rangle + \cdots + a_{N-1} |N-1\rangle$
 $= a_0 |0 \cdots 0\rangle + \cdots + a_{N-1} |1 \cdots 1\rangle$
 $= \begin{bmatrix} a_0 \\ \vdots \\ a_{N-1} \end{bmatrix}.$
- Concatenando registradores;
 $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle |\phi\rangle = |\psi, \phi\rangle = |\psi\phi\rangle.$
- Vetor dual $\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^*)^T$;
 $\langle\psi| = a_0^* \langle 0| + \cdots + a_{N-1}^* \langle N-1|$
 $= a_0^* \langle 0 \cdots 0| + \cdots + a_{N-1}^* \langle 1 \cdots 1|$
 $= \begin{bmatrix} a_0^* & \cdots & a_{N-1}^* \end{bmatrix}.$

- Vetores unitários $|\psi\rangle \in \mathcal{H}^N$, $N = 2^n$;
 $|\psi\rangle = a_0 |0\rangle + \dots + a_{N-1} |N-1\rangle$
 $= a_0 |0 \dots 0\rangle + \dots + a_{N-1} |1 \dots 1\rangle$
 $= \begin{bmatrix} a_0 \\ \vdots \\ a_{N-1} \end{bmatrix}.$

- Concatenando registradores;
 $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle |\phi\rangle = |\psi\phi\rangle.$
- Vetor dual $\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^*)^T$;
 $\langle\psi| = a_0^* \langle 0| + \dots + a_{N-1}^* \langle N-1|$
 $= a_0^* \langle 0 \dots 0| + \dots + a_{N-1}^* \langle 1 \dots 1|$
 $= \begin{bmatrix} a_0^* & \dots & a_{N-1}^* \end{bmatrix}.$

Cursos
FMC
AL
OAC

Definições – Matrizes

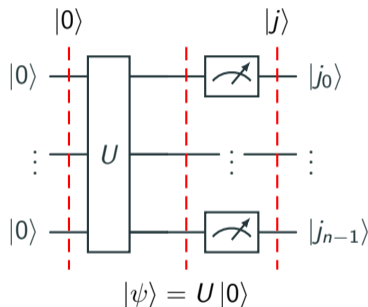
- Usando *ket* e *bra*;
 - Produto interno $\langle \psi | \phi \rangle$;
 - Produto externo $|\psi\rangle \langle \phi|$.

- Matrizes unitárias U ;

$$U = \begin{bmatrix} U_{00} & \cdots & U_{0(N-1)} \\ \vdots & \ddots & \vdots \\ U_{(N-1)0} & \cdots & U_{(N-1)(N-1)} \end{bmatrix}$$
$$= \sum_{ij} U_{ij} |i\rangle \langle j|.$$

- Medição;

- 1) $|\psi\rangle = a_0 |0\rangle + \cdots + a_{N-1} |N-1\rangle$;
- 2) $|j\rangle$ com prob. $|a_j|^2$.



Cursos

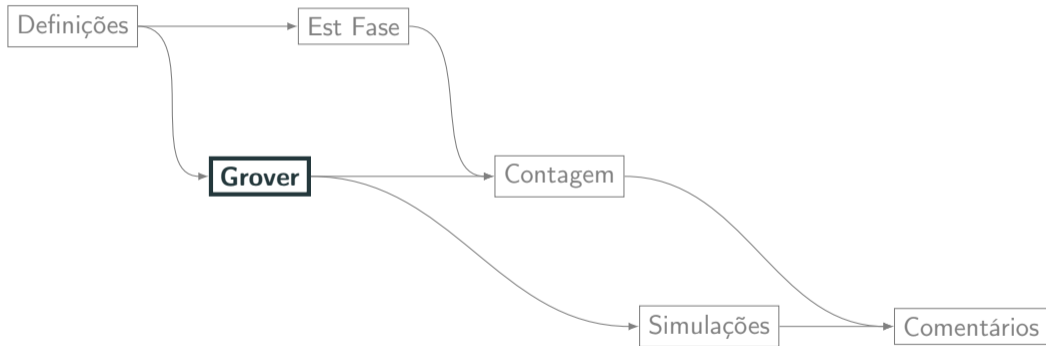
FMC

AL

Circ

OAC

Prob



- Consultas a um oráculo Q .
 - Q como (ponteiro de) função.
- Busca em lista ordenada $O(\log N)$;
- Busca em lista desordenada;
 - Clássico: $O(N)$;
 - Quântico: $O(\sqrt{N})$.

Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

Algr

- Oráculo Q ;

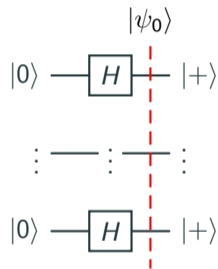
$$Q : |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle ,$$

- Palpite inicial;

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_j |j\rangle$$

- Como implementar?

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



Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

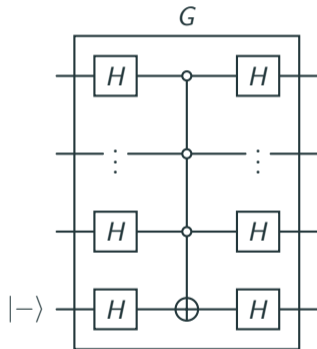
Algr

Grover – Operador

- Operador de Grover;

$$G = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$$

$$= \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{bmatrix}.$$



Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

Algr

Grover – Primeira iteração

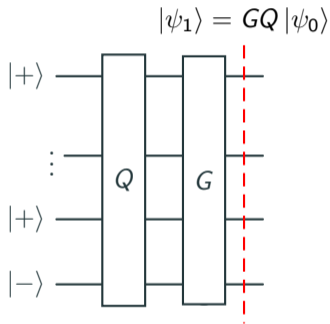
- Marcado $|m\rangle$;

- Não marcados

$$|\bar{m}\rangle = \frac{1}{\sqrt{N-1}} \sum_{j \neq m} |j\rangle$$

- Reescrever $|\psi_0\rangle$;

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} |m\rangle + \frac{\sqrt{N-1}}{\sqrt{N}} |\bar{m}\rangle.$$



Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

Algr

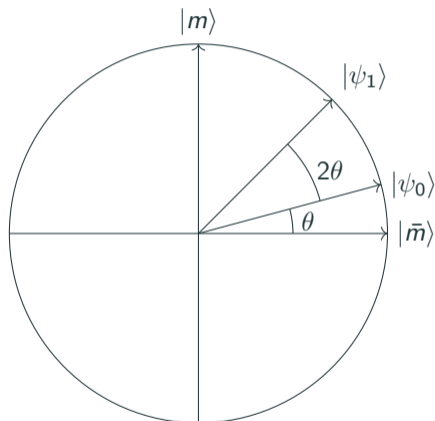
Grover – Primeira iteração

- $|\psi_0\rangle$ no hiperplano;

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{N}} |m\rangle + \frac{\sqrt{N-1}}{\sqrt{N}} |\bar{m}\rangle \\ &= \sin \theta |m\rangle + \cos \theta |\bar{m}\rangle \end{aligned}$$

- $|\psi_1\rangle$ no hiperplano;

$$\begin{aligned} |\psi_1\rangle &= GQ |\psi_0\rangle \\ &= \sin(3\theta) |m\rangle + \cos(3\theta) |\bar{m}\rangle \end{aligned}$$



Cursos

FMC

AL

Circ

OAC

Prob

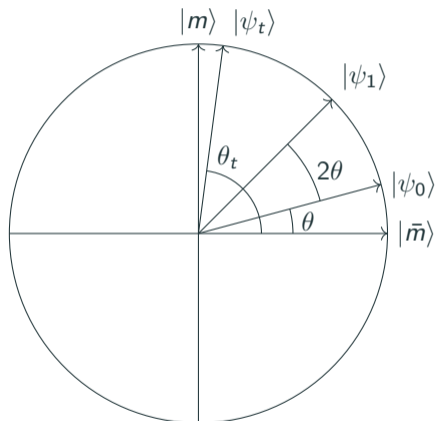
EDB

Prog

Algr

Grover – t -ésima iteração

- $|\psi_t\rangle$ no hiperplano, $\theta_t = (2t + 1)\theta$;
 $|\psi_t\rangle = (GQ)^t |\psi_0\rangle$
 $= \sin \theta_t |m\rangle + \cos \theta_t |\bar{m}\rangle$
- Parar quando $|\psi_t\rangle \approx |m\rangle$;
- $N \rightarrow \infty \implies \theta = 1/\sqrt{N} \approx 0$;
- Logo,
$$(2t + 1) \frac{1}{\sqrt{N}} \approx \frac{\pi}{2} \implies t \approx \frac{\pi\sqrt{N}}{4}.$$



Cursos

FMC

AL

Circ

OAC

Prob

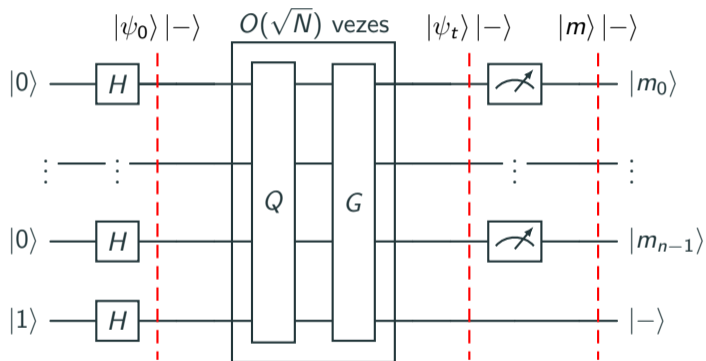
EDB

Prog

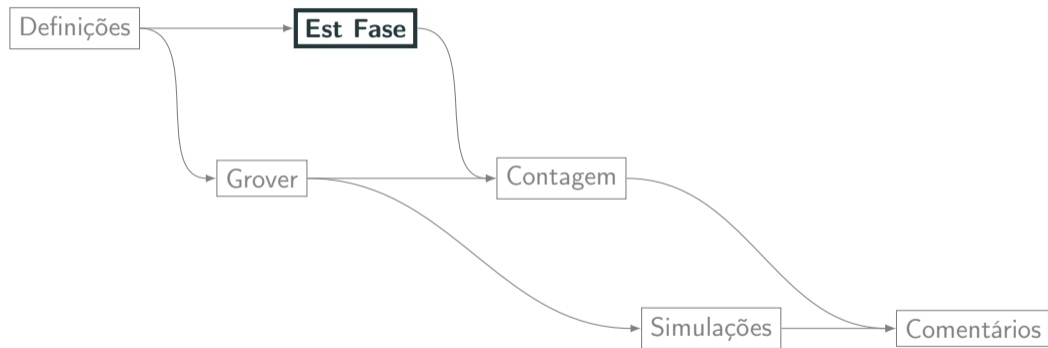
Algr

Calc

Grover – Circuito Final



Estimativa de Fase



- Dado um $e^{i2\pi\lambda}$ -autovetor $|\lambda\rangle$ de U ;
 $U|\lambda\rangle = (\cos(2\pi\lambda) + i\sin(2\pi\lambda))|\lambda\rangle$.
- Estimar λ .

Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

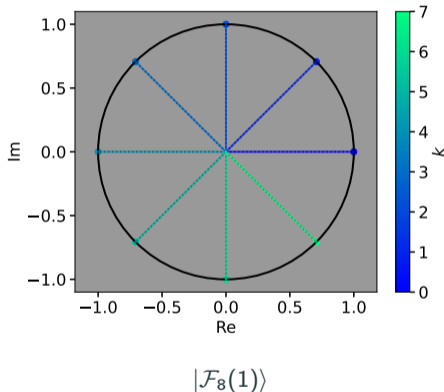
Algr

Calc

Estimativa de Fase – QFT

- Dado um $e^{i2\pi\lambda}$ -autovetor $|\lambda\rangle$ de U ;
 $U|\lambda\rangle = (\cos(2\pi\lambda) + i\sin(2\pi\lambda))|\lambda\rangle$.
- Estimar λ .
- Transformada de Fourier Quântica;
QFT $|j\rangle = |\mathcal{F}_P(j)\rangle$

$$= \frac{1}{\sqrt{P}} \sum_{k=0}^{P-1} \exp\left(2\pi i \frac{jk}{P}\right) |k\rangle.$$



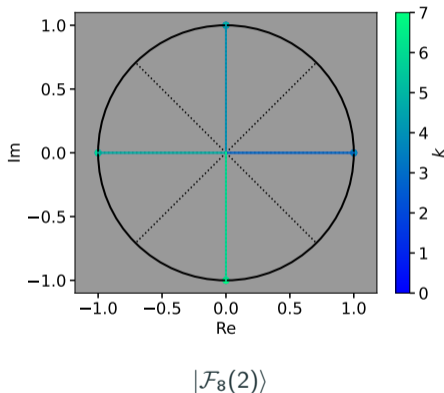
Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc

Estimativa de Fase – QFT

- Dado um $e^{i2\pi\lambda}$ -autovetor $|\lambda\rangle$ de U ;
 $U|\lambda\rangle = (\cos(2\pi\lambda) + i\sin(2\pi\lambda))|\lambda\rangle$.
- Estimar λ .
- Transformada de Fourier Quântica;
QFT $|j\rangle = |\mathcal{F}_P(j)\rangle$

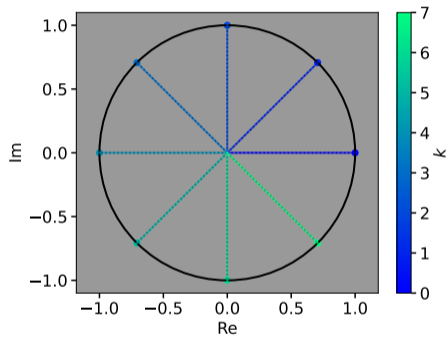
$$= \frac{1}{\sqrt{P}} \sum_{k=0}^{P-1} \exp\left(2\pi i \frac{jk}{P}\right) |k\rangle.$$



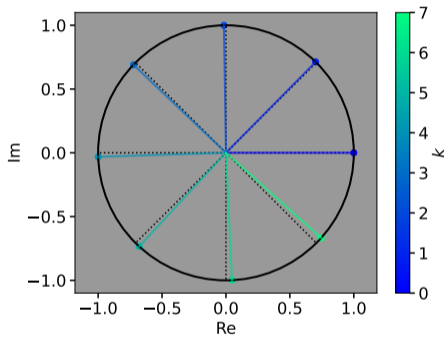
Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc

Estimativa de Fase – QFT



$|\mathcal{F}_8(1)\rangle$



$|\mathcal{F}_8(1.01)\rangle$

Cursos

FMC

AL

Circ

OAC

Prob

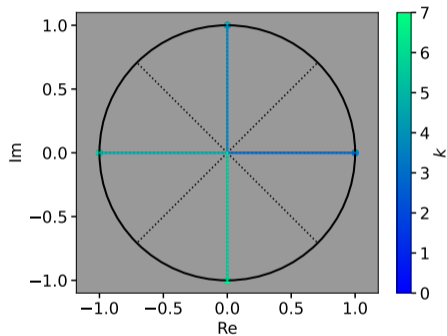
EDB

Prog

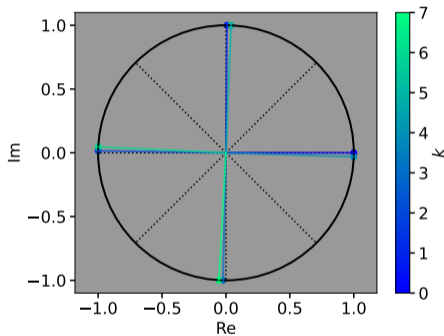
Algr

Calc

Estimativa de Fase – QFT



$|\mathcal{F}_8(2)\rangle$



$|\mathcal{F}_8(1.99)\rangle$

Cursos

FMC

AL

Circ

OAC

Prob

EDB

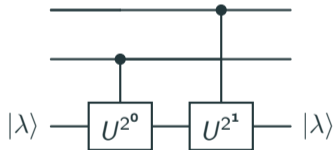
Prog

Algr

Calc

Estimativa de Fase – Circuito

- $QFT |j\rangle = |\mathcal{F}_P(j)\rangle$
- $QFT^\dagger |\mathcal{F}_P(j)\rangle = |j\rangle$
- Conseguimos obter $|\mathcal{F}_P(P\lambda)\rangle$?



- $|00\rangle |\lambda\rangle \rightarrow |00\rangle |\lambda\rangle$;
- $|01\rangle |\lambda\rangle \rightarrow \exp(2\pi i\lambda) |01\rangle |\lambda\rangle$;
- $|10\rangle |\lambda\rangle \rightarrow \exp(2\pi i2\lambda) |10\rangle |\lambda\rangle$;
- $|11\rangle |\lambda\rangle \rightarrow \exp(2\pi i3\lambda) |11\rangle |\lambda\rangle$;

Cursos

FMC

AL

Circ

OAC

Prob

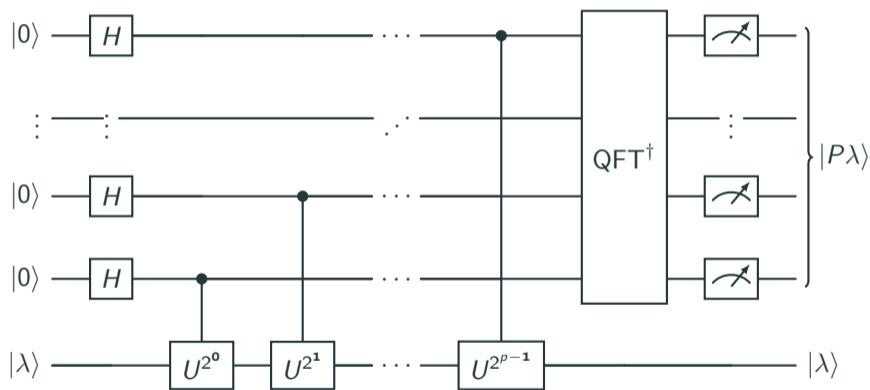
EDB

Prog

Algr

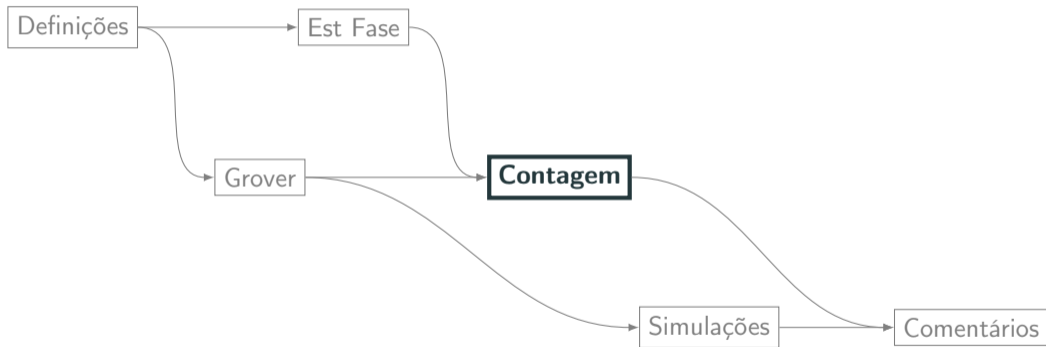
Calc

Estimativa de Fase – Circuito



Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc



- Conjunto M de marcados;
- 1 marcado $\rightarrow |M|$ marcados;
- Busca $O(\sqrt{N/|M|})$;
- Contar antes de buscar.

- $|m\rangle \rightarrow |M\rangle$;
$$|M\rangle = \frac{1}{\sqrt{|M|}} \sum_{m \in M} |m\rangle.$$
- $|\bar{m}\rangle \rightarrow |\bar{M}\rangle$;
$$|\bar{M}\rangle = \frac{1}{\sqrt{N - |M|}} \sum_{\bar{m} \in \bar{M}} |\bar{m}\rangle.$$

Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc
Conj

- $|\psi_0\rangle$ no hiperplano:

$$\begin{aligned} |\psi_0\rangle &= \sqrt{\frac{|M|}{N}} |M\rangle + \sqrt{\frac{N - |M|}{N}} |\bar{M}\rangle \\ &= \cos\theta |M\rangle + \sin\theta |\bar{M}\rangle. \end{aligned}$$

- GQ é uma matriz de rotação;

$$GQ_{\text{red}} = \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix}$$

- $e^{\pm i2\theta}$ -autovetores

$$|\mp i\rangle = \frac{|\bar{M}\rangle \mp i|M\rangle}{\sqrt{2}}$$

- Estimar $\theta \implies$ estimar $|M|$;

- Como obter $|\mp i\rangle$?

$$|\psi_0\rangle = \frac{e^{i\theta}}{\sqrt{2}} |-i\rangle + \frac{e^{-i\theta}}{\sqrt{2}} |+i\rangle.$$

Cursos

FMC

AL

Circ

OAC

Prob

EDB

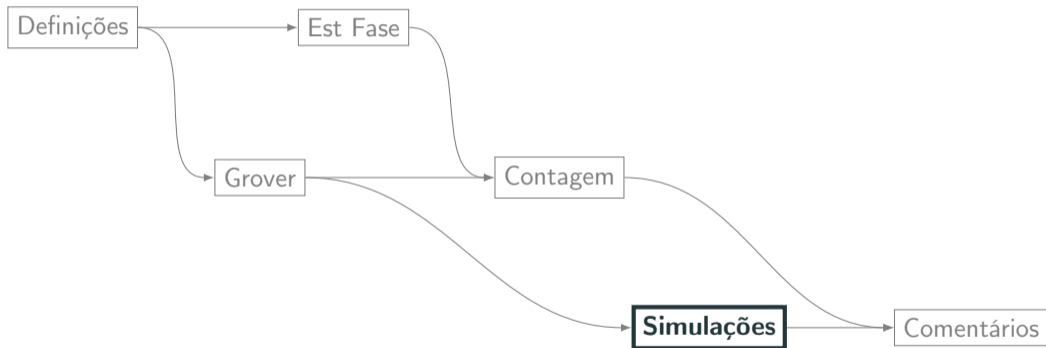
Prog

Algr

Calc

Conj

VGA



- Computadores quânticos;
 - Ruidosos;
 - $1000 \rightarrow 1$;
 - Acesso limitado;
 - Difícil implementação.
- Computadores clássicos;
 - Obter intuição;
 - Prova de conceito;
 - Implementação mais fácil;
 - Requer muita memória.

Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc
Conj

Simulações – Santos Dumont







- 1) LabInfo - Bioinformática;
- 2) GMMSB - Modelagem Molecular de Sistemas Biológicos;
- 3) BAMC - Biologia Aplicada à Modelagem Matemática e Computacional;
- 4) HeMoLab - Laboratório de Modelagem em Hemodinâmica;
- 5) TMC - Modelagem Computacional do Crescimento Tumoral;
- 6) COMOPORE - Modelagem Computacional de Materiais Porosos;
- 7) IPES - Innovative Parallel Finite Element Solvers;
- 8) MIE - Modelagem de Incertezas Epistêmicas;
- 9) ESDA - Estabilização de Sistemas Dinâmicos e Aplicações;
- 10) **GCQC - COMPUTAÇÃO QUÂNTICA E CRIPTOGRAFIA;**
- 11) DEXL - Data Extreme Lab;
- 12) CAD - Computação de Alto Desempenho;
- 13) ACiMA - Ambientes Colaborativos e Multimídia Aplicada;
- 14) PIVC - Processamento de Imagens e Visualização Científica;
- 15) ComCiDis - Computação Científica Distribuída;
- 16) GCON - Sistemas e Controle.

hiperwalk.org | 

Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

Algr

Calc

Conj

Grafos

LFA

EngSoft

ParDist

Cursos

FMC

AL

Circ

OAC

Prob

EDB

Prog

Algr

Calc

Conj

Grafos

LFA

EngSoft

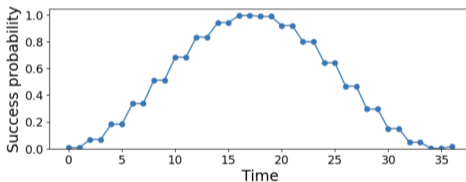
ParDist

Try Hiperwalk

Use the interactive shell to try Hiperwalk in the browser

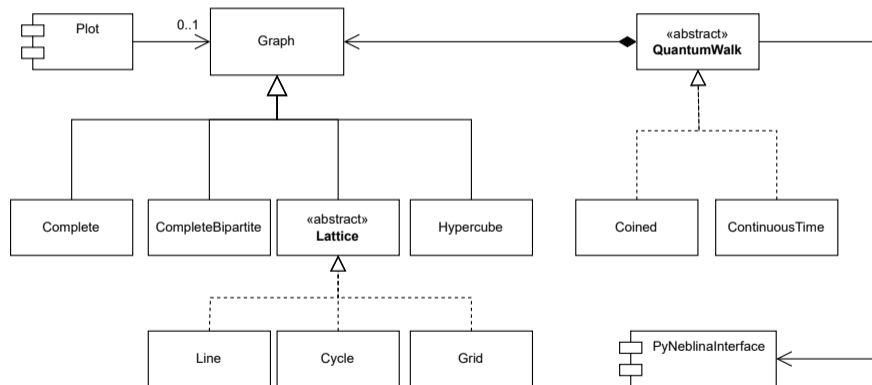
```
import hiperwalk as hpw
import numpy as np

N = 128
# adjacency matrix of complete graph with self loops
A = np.ones((N, N))
graph = hpw.Graph(A)
qw = hpw.Coined(graph,
                shift='flipflop',
                coin='G',
                marked={'-G': [0]})
t_final = (round(4*np.pi*np.sqrt(N)/4),1)
states = qw.simulate(time=t_final,
                    state=qw.uniform_state())
marked_prob = qw.success_probability(states)
hpw.plot_success_probability(t_final,
                            marked_prob,
                            figsize=(9,3))
```



[1]

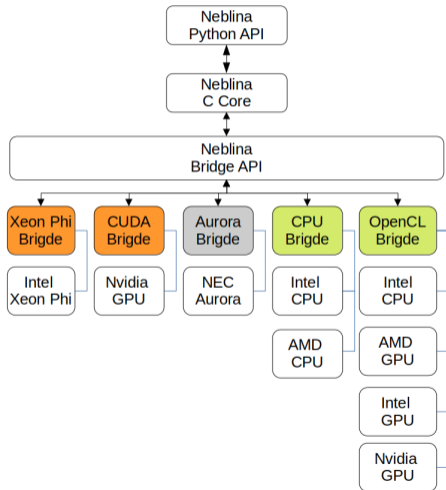
Simulações – Hiperwalk – Arquitetura



Cursos

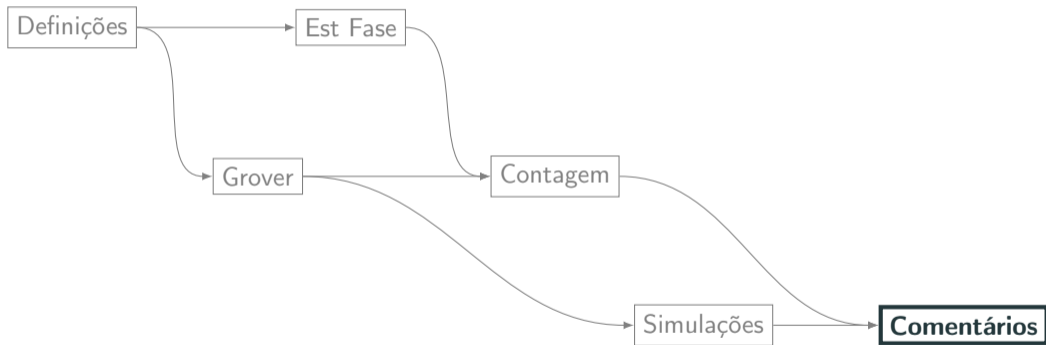
- FMC
- AL
- Circ
- OAC
- Prob
- EDB
- Prog
- Algr
- Calc
- Conj
- Grafos
- LFA
- EngSoft
- ParDist

Simulações – Hiperwalk – HiperBLAS



Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc
Conj
Grafos
LFA
EngSoft
ParDist



- Muitos outros algoritmos;
 - Shor;
 - HHL;
 - Distinção de elementos;
 - Busca em grafos;
- Trabalhos em outras áreas;
 - Otimização;
 - Inteligência artificial;
 - Algoritmos distribuídos;
- Abrange todas as áreas da computação.

Cursos

FMC
AL
Circ
OAC
Prob
EDB
Prog
Algr
Calc
Conj
Grafos
LFA
EngSoft
⋮

Obrigado!

gustavowl.github.io