Hands on Quantum Mechanics Quantum Computing

Mariana Gama - 78731
João Gonçalves - 75956

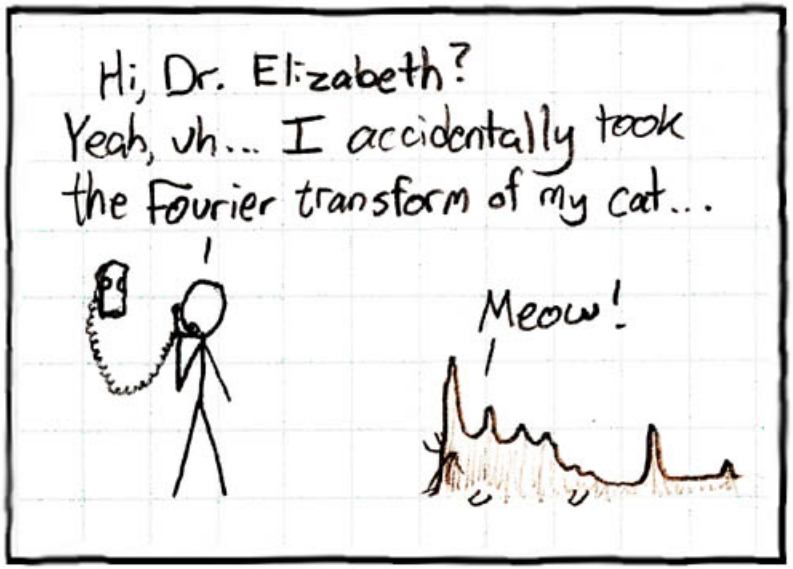
MEFT
2016

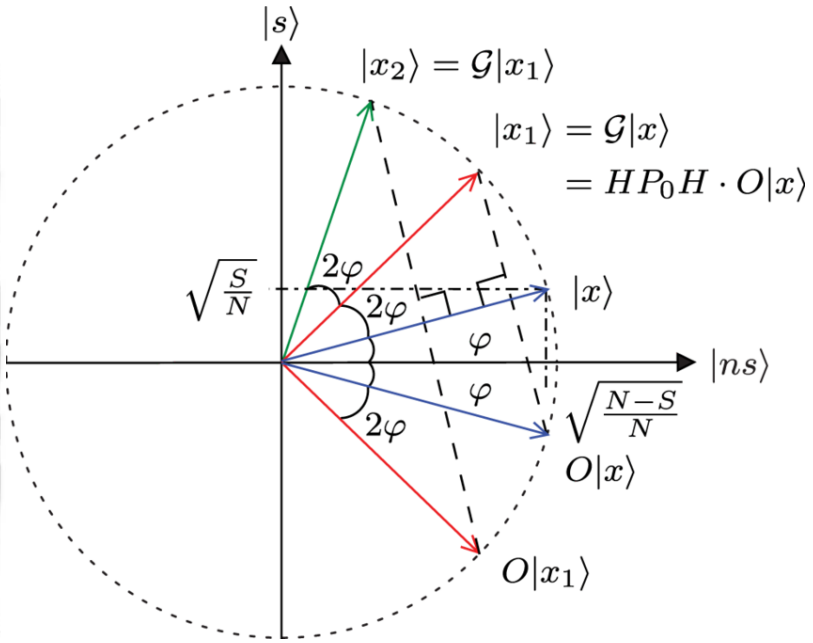
Professor Filipe Joaquim

Índice

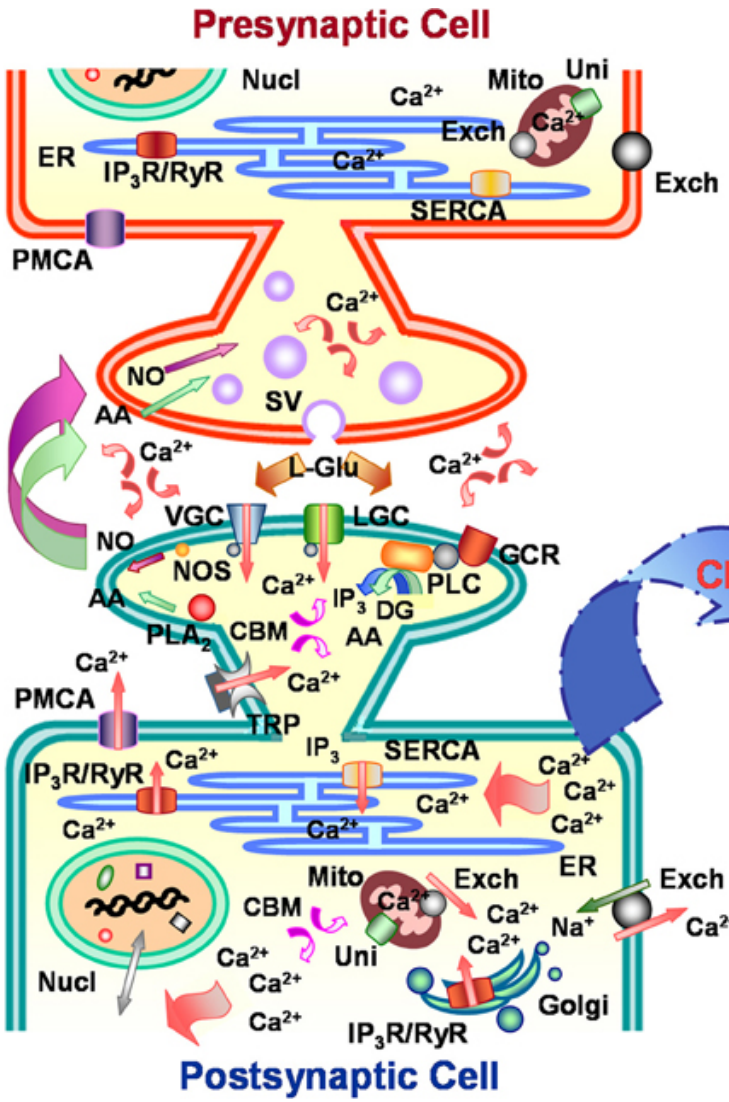
Recomeçando...
O que vos vamos falar.
Mas porquê?
Transformada de Fourier quântica
Motivação
RSA Cryptosystem
O Circuito
Fases
Algoritmos de procura quântica
O problema
O oráculo
Para RSA
O procedimento
A iteração de Grover
Visualização geométrica
Conclusões

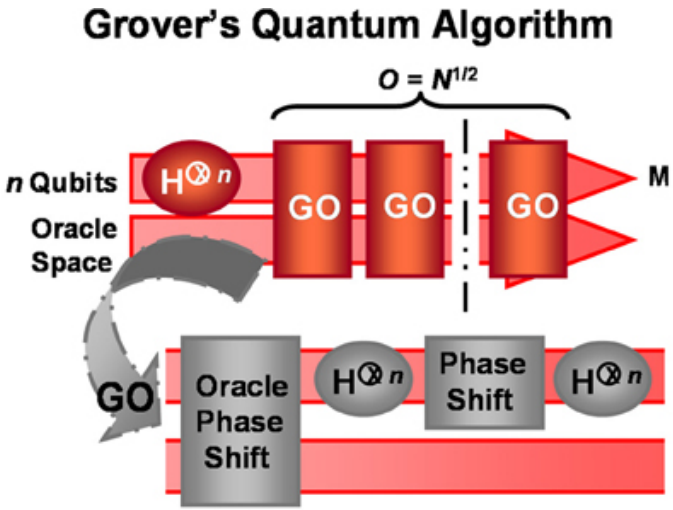
O que vos vamos falar.

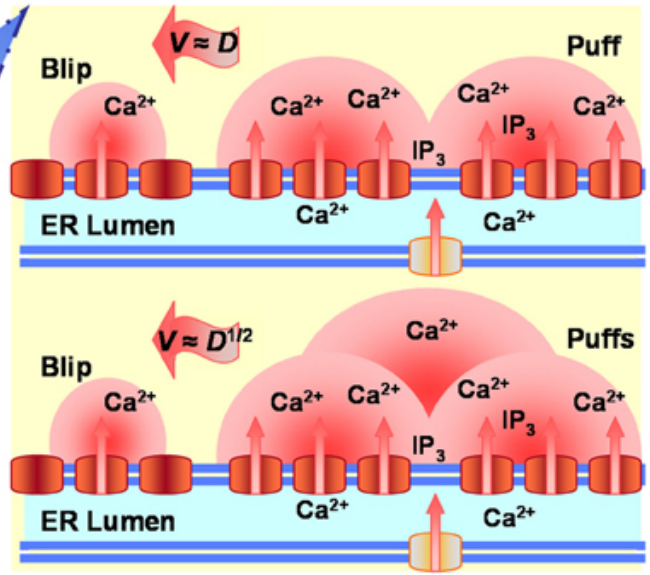




Mas porquê?







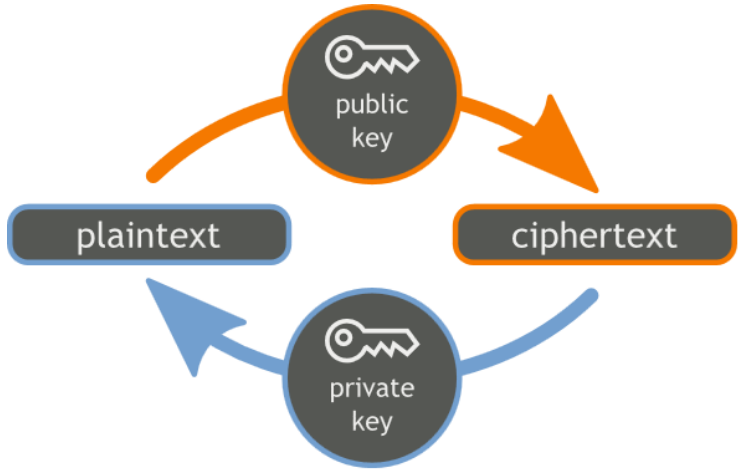
http://journal.frontiersin.org/article/10.3389/fnmol.2014.00029/full

Índice

Motivação

Sistema RSA e Algoritmo de Shor

1. Escolher dois números primos grandes p e q $(eg: p = 61, q = 53)$.
2. Calcular o produto $n = pq$ $(n = 3233)$.
3. Escolher um inteiro pequeno, e, coprimo com $\varphi(n) = (p-1)(q-1)$ $(e = 17)$.
4. Calcular d, o inverso multiplicativo de e módulo $\varphi(n)$ $(d = 2753)$.
5. A *chave pública RSA* é o par $P = (e, n)$. A *chave privada RSA* é o par $S = (d, n)$



Algoritmo para T. Fourier

A transformada de Fourier quântica é definida como:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

Com alguns cálculos...

$$\begin{aligned}
|j\rangle \rightarrow & \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \\
= & \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \ldots k_n\rangle \\
= & \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
= & \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
= & \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \\
= & \frac{\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n} |1\rangle\right)}{2^{n/2}}
\end{aligned}$$

Circuito para T. Fourier

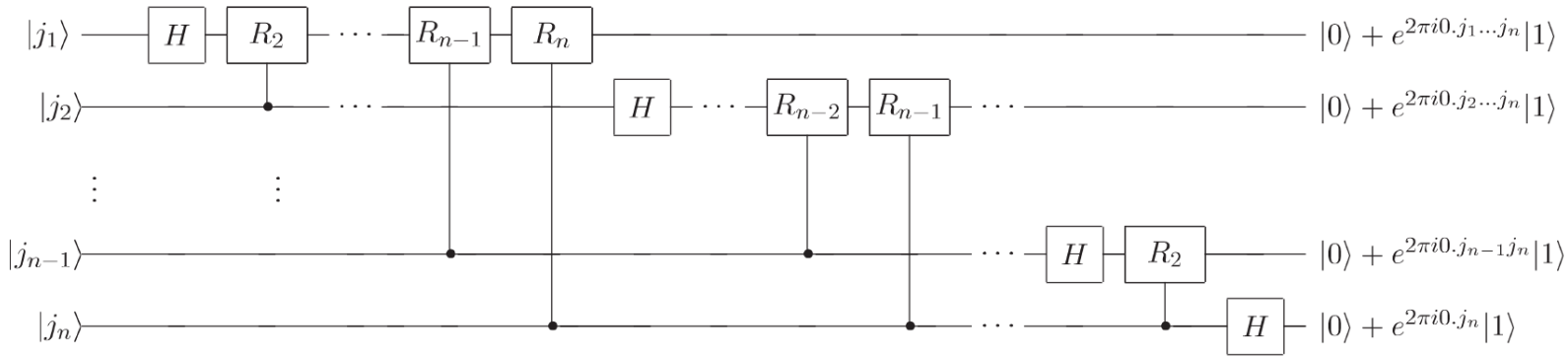
Podemos então representar a transformada de Fourier como:

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

em que $0.j_l j_{l+1}...j_m$ representa a *fracção binária* $j_l/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$.

Utilizando portas de Hadamard e portas R_k, obtemos assim um circuito que efectua a transformada de Fourier quântica.

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$



T. Fourier para estimação de fases

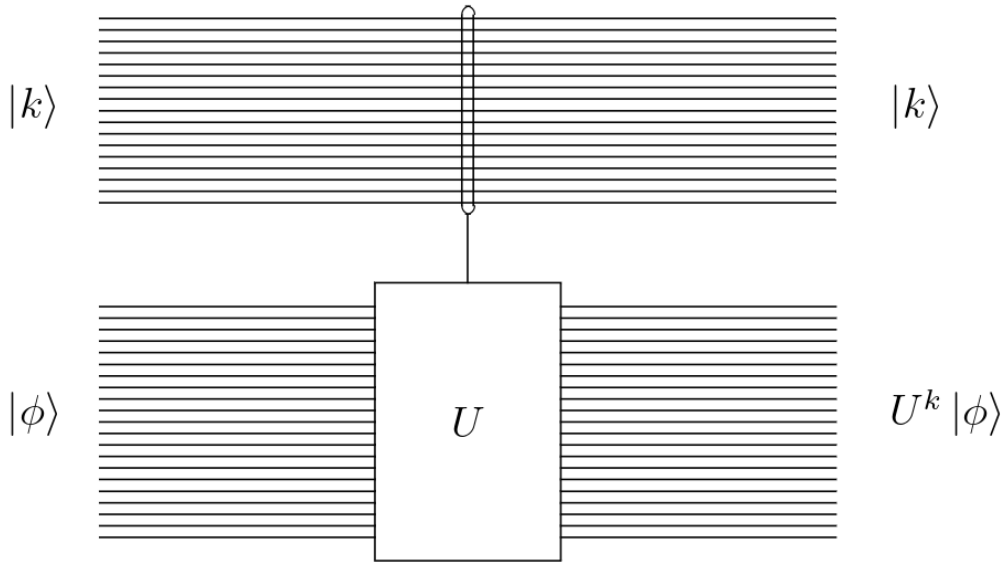
O problema da estimação de fases prende-se com a obtenção de $\theta \in [0, 1)$, resultante da aplicação de uma transformação U a um estado próprio ψ:

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

Para resolver o problema, vamos aplicar a seguinte operação:

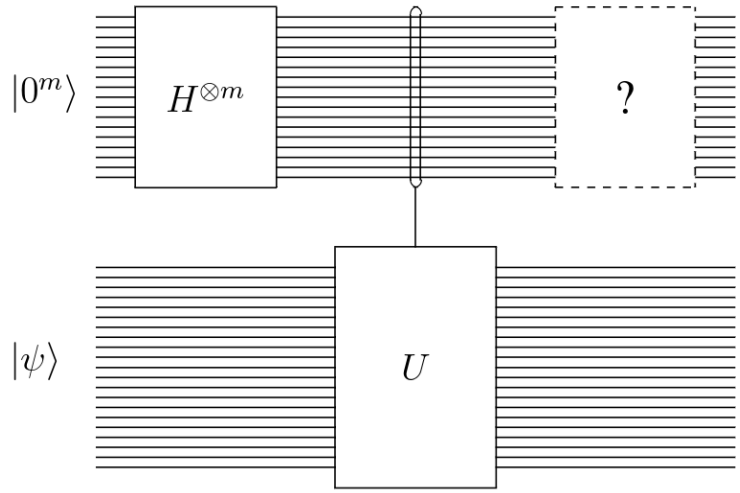
$$\Lambda_m(U) |k\rangle |\phi\rangle = |k\rangle \left(U^k |\phi\rangle\right)$$

Representada esquematicamente como:



T. Fourier para estimação de fases

Considerando o circuito seguinte,



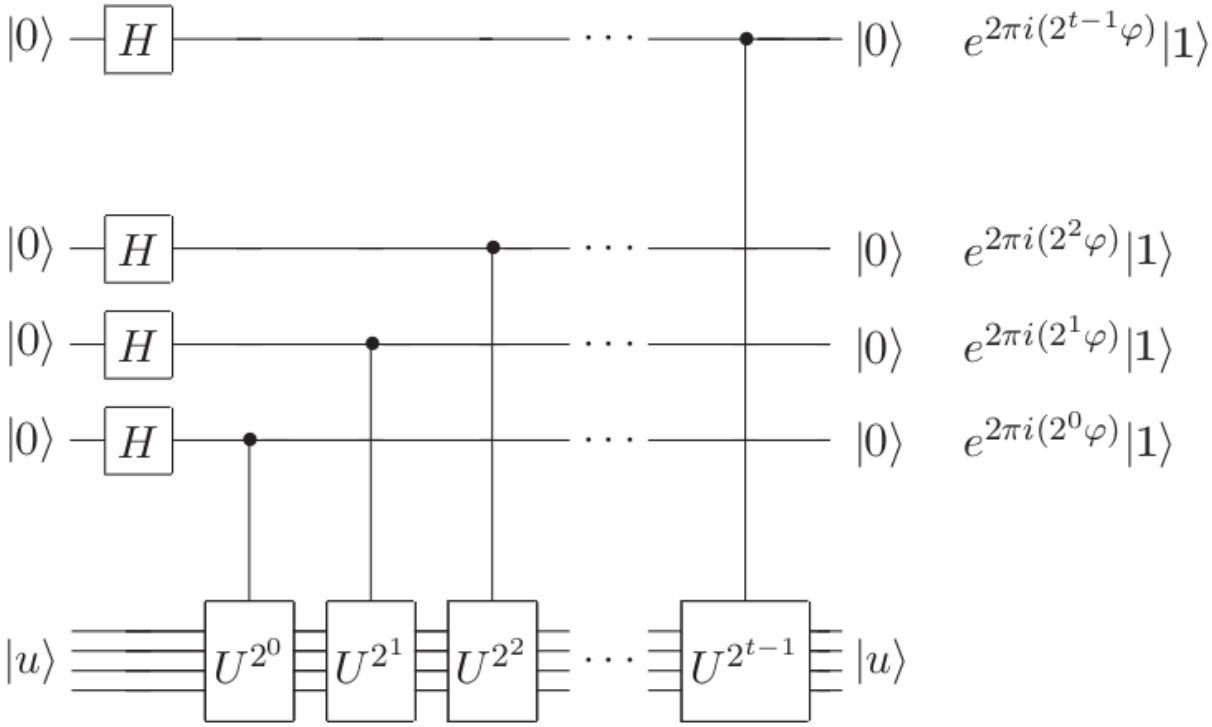
$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle |\psi\rangle .$$

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle \left(U^k |\psi\rangle\right)$$

$$U^k |\psi\rangle = \left(e^{2\pi i\theta}\right)^k |\psi\rangle = e^{2\pi ik\theta} |\psi\rangle$$

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle \left(e^{2\pi ik\theta} |\psi\rangle\right) = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} e^{2\pi ik\theta} |k\rangle |\psi\rangle$$

T. Fourier para estimação de fases



Os primeiros qbits vão corresponder à transformada de Fourier da fase que queremos obter!

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j} |j\rangle |u\rangle \rightarrow |\tilde{\varphi}\rangle |u\rangle$$

Estimação de Fases: Aplicações

Order Finding e Factorização

Order finding: encontrar r tal que $x^r \equiv 1 \bmod N$ para $x < N$

O problema da factorização pode ser reduzido a order finding!

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.

- Jennifer and Peter Shor

Índice

O problema

- Queremos fazer uma procura num espaço de N elementos;
- Vamos trabalhar com os índices associados a estes elementos;
- Assume-se $N = 2^n$ pelo que o índice é guardado em n bits;
- A procura tem M soluções tal que: $0 \leq M \leq N$;
- Definimos uma função $f(x)$ que recebe um inteiro x ente 0 e $N - 1$;
- Fazemos com que se $f(x) = 1$ x é uma solução e é 0 caso contrário;

O oráculo

O oráculo

$$|x\rangle |q\rangle \xrightarrow{O} |x\rangle |q \oplus f(x)\rangle$$

.

O oráculo

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

.

O oráculo

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right)$$

.

O oráculo

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

.

O oráculo

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

.

O oráculo

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

Parece que o oráculo apenas faz uma inversão de fase ao índice testado caso este seja uma solução

.

O oráculo

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

Parece que o oráculo apenas faz uma inversão de fase ao índice testado caso este seja uma solução

.

Clássico vs Quântico

O oráculo

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

Parece que o oráculo apenas faz uma inversão de fase ao índice testado caso este seja uma solução

.

Clássico vs Quântico

$$O(N/M) \text{ vs } O(\sqrt{N/M})$$

O oráculo

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

Parece que o oráculo apenas faz uma inversão de fase ao índice testado caso este seja uma solução

.

Clássico vs Quântico

$$O(N/M) \text{ vs } O(\sqrt{N/M})$$

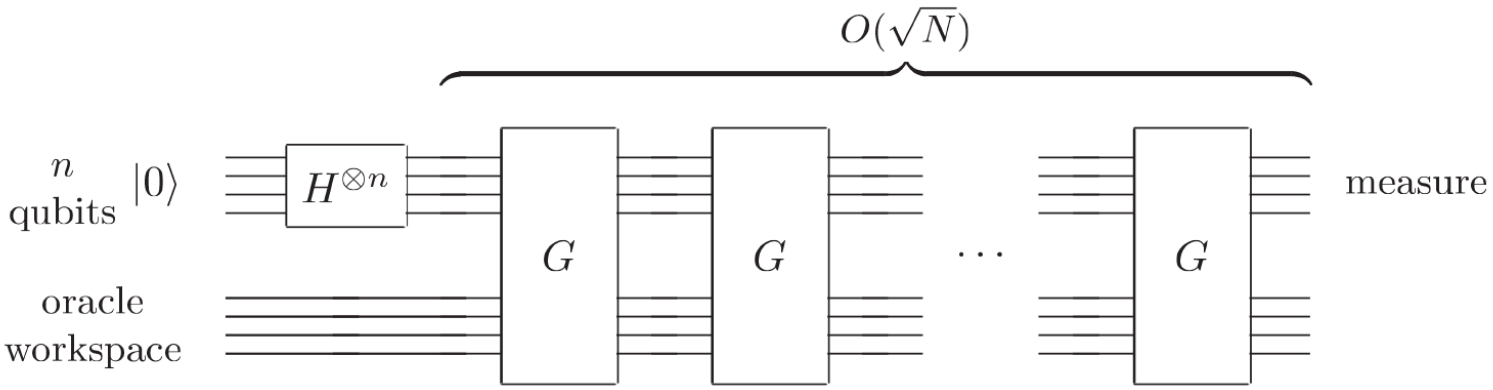
Mas João o oráculo parece que sabe, a priori, as soluções do problema. De que me serve um algoritmo para resolver um problema se este precisa de saber as soluções a princípio?

O oráculo

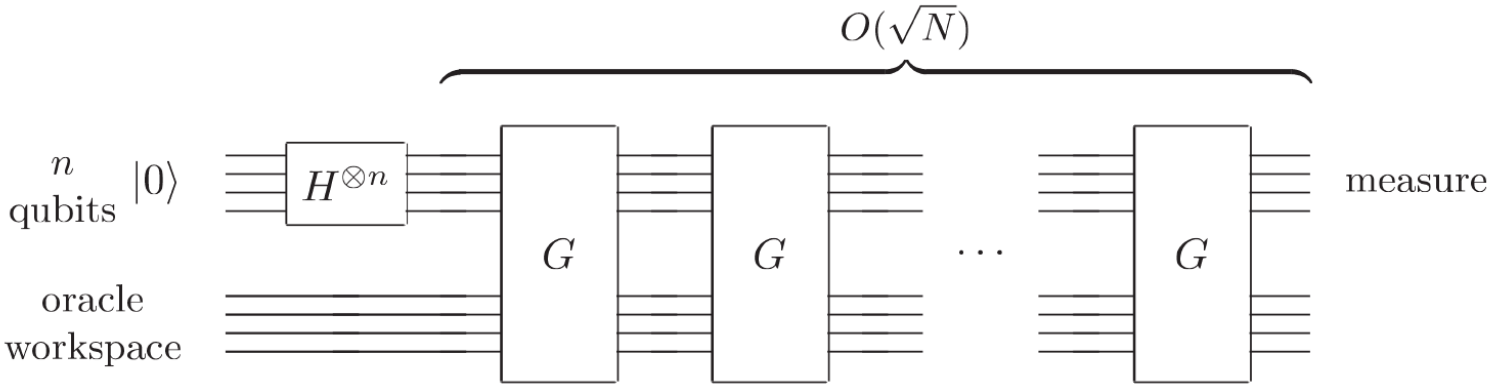
Para RSA

http://thehackernews.com/2013/12/nsa-paid-10-million-bribe-to-rsa.html

O procedimento

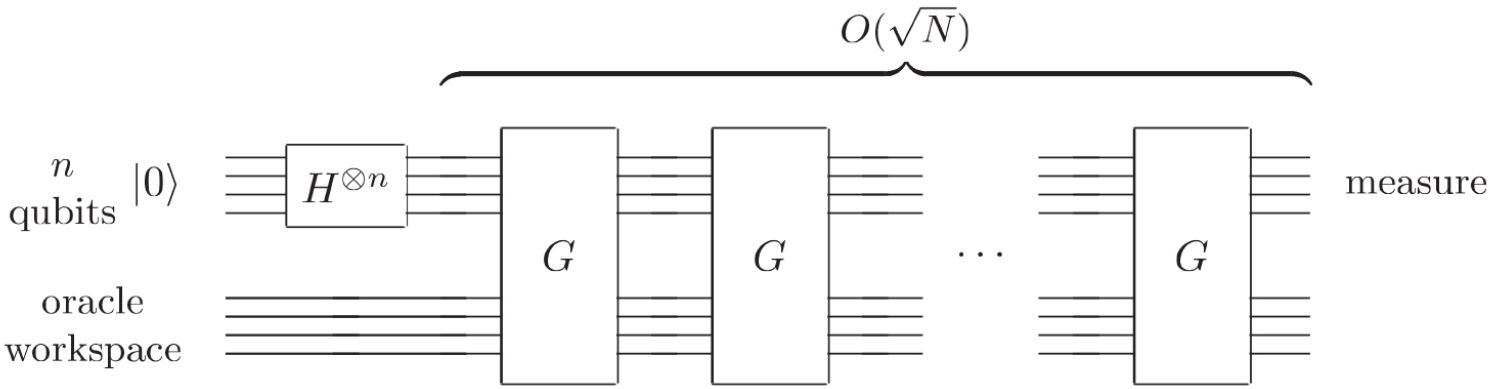


O procedimento



$$|\Psi_0\rangle = |0\rangle^{\otimes n}$$

O procedimento

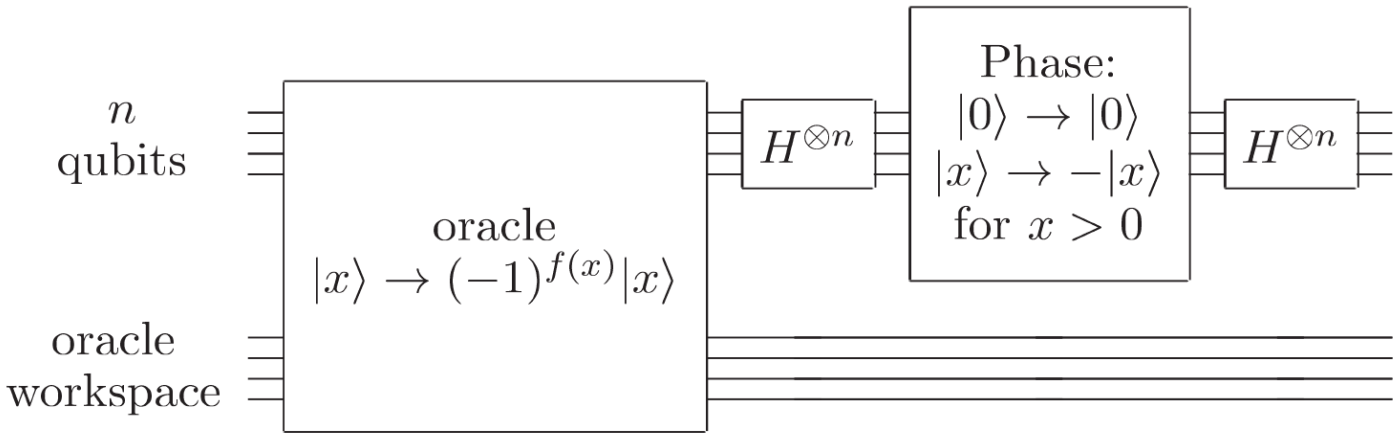


$$|\Psi_0\rangle = |0\rangle^{\otimes n}$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

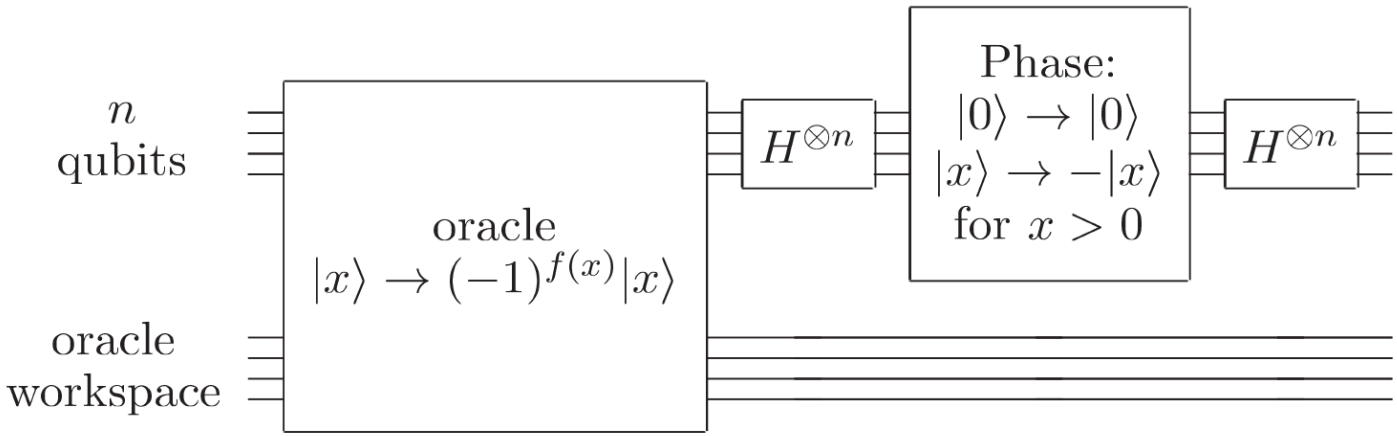
O procedimento

A iteração de Grover



O procedimento

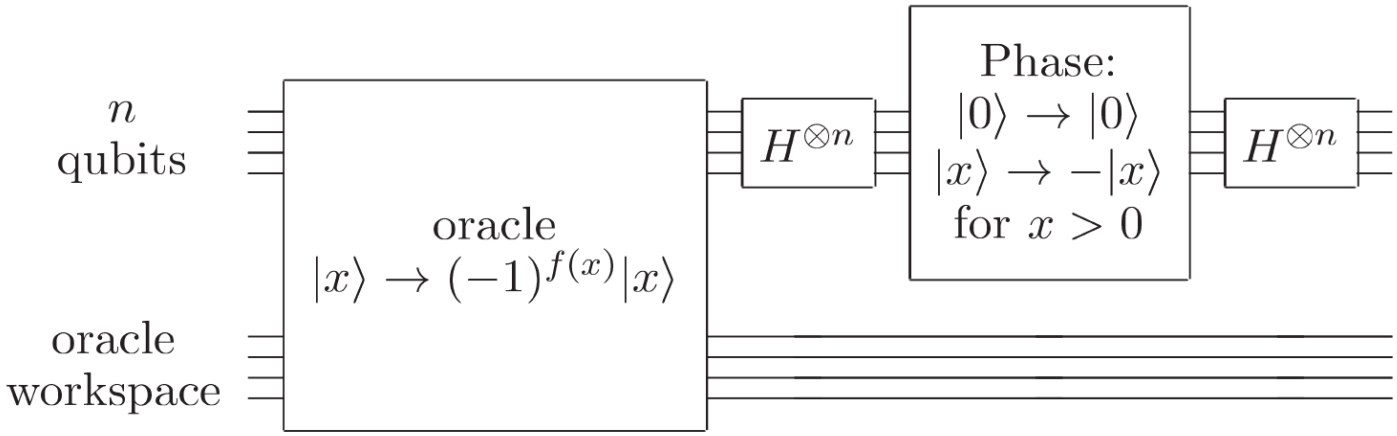
A iteração de Grover



- Aplicar o oráculo;

O procedimento

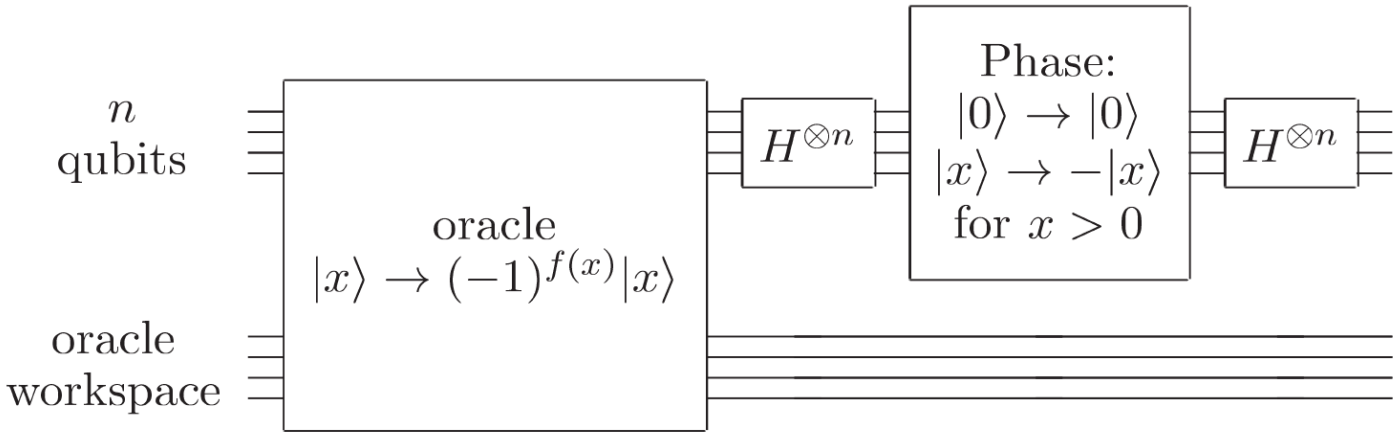
A iteração de Grover



- Aplicar o oráculo;
- Aplicar a transformada de Hadamard;

O procedimento

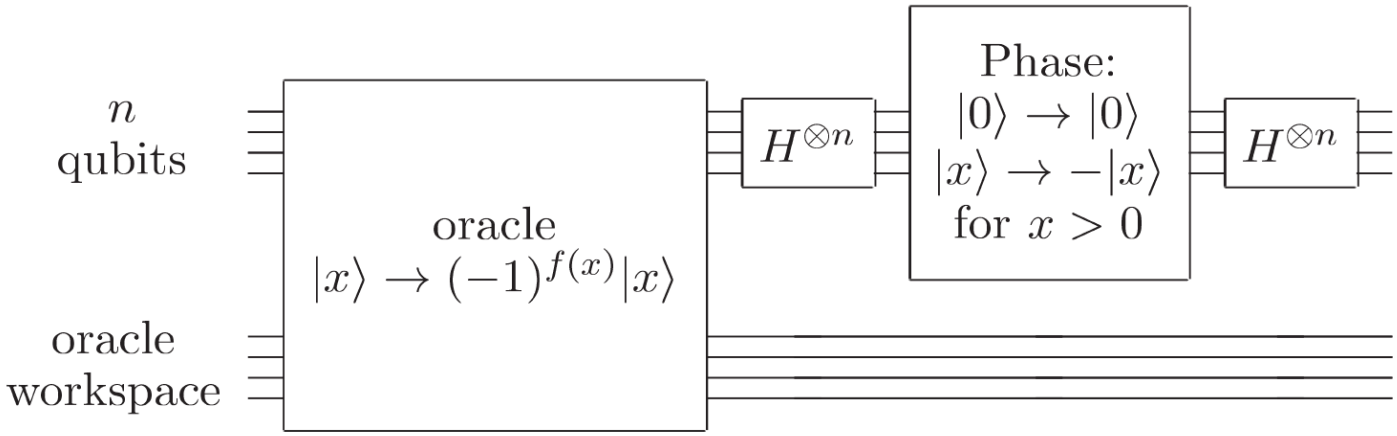
A iteração de Grover



- Aplicar o oráculo;
- Aplicar a transformada de Hadamard;
- Aplicar a inversão de fase condicional;

O procedimento

A iteração de Grover

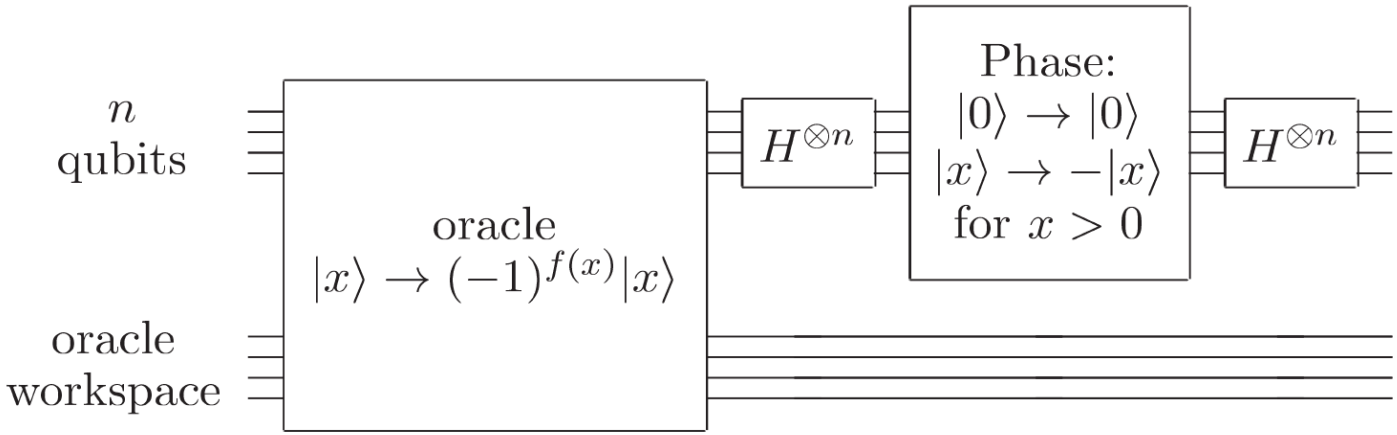


- Aplicar o oráculo;
- Aplicar a transformada de Hadamard;
- Aplicar a inversão de fase condicional;

$$|x\rangle \to -(-1)^{\delta_{x0}} |x\rangle$$

O procedimento

A iteração de Grover



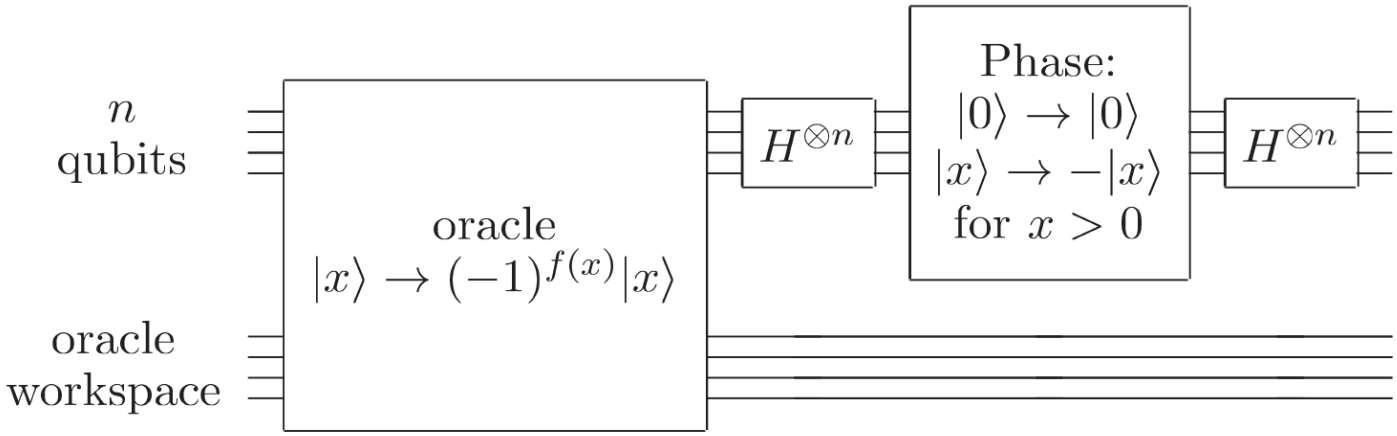
- Aplicar o oráculo;
- Aplicar a transformada de Hadamard;
- Aplicar a inversão de fase condicional;

$$|x\rangle \to -(-1)^{\delta_{x0}} |x\rangle$$

- Aplicar de novo a transformada de Hadamard;

O procedimento

A iteração de Grover

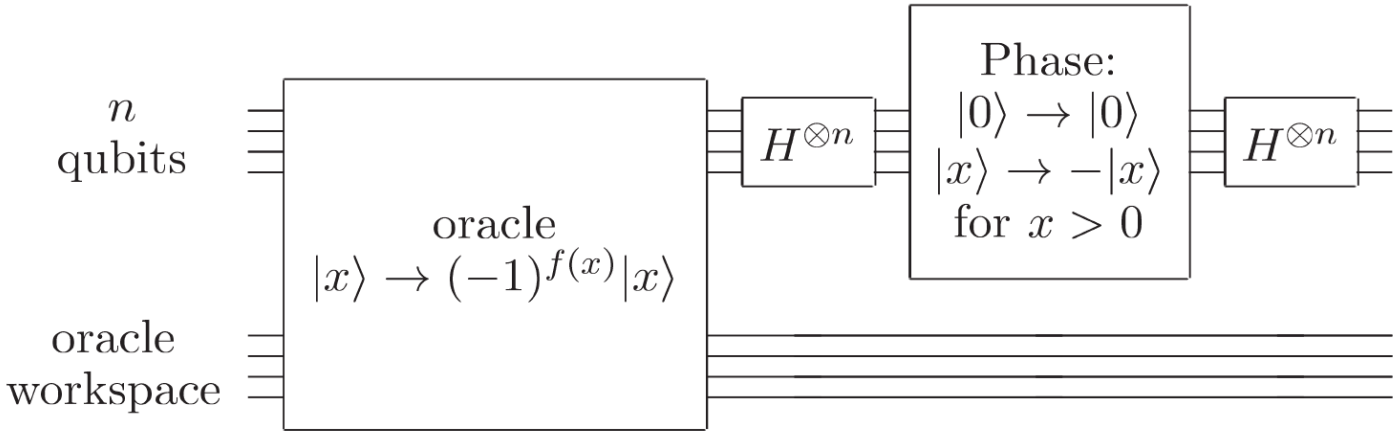


Olhando para os três útlimos passos temos:

$$H^{\otimes n}(2\,|0\rangle\,\langle 0| - I)H^{\otimes n} = 2\,|\Psi_1\rangle\,\langle\Psi_1| - I$$

O procedimento

A iteração de Grover



Olhando para os três útlimos passos temos:

$$H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right| - I)H^{\otimes n} = 2\left|\Psi_1\right\rangle\left\langle\Psi_1\right| - I$$

Por fim temos o operador de Grover:

$$G = (2\left|\Psi_1\right\rangle\left\langle\Psi_1\right| - I)O$$

- Comecemos por definir $\sum_x'$ como a soma sobre todos os x que são solução e $\sum_x''$, como a soma sobre os restantes x.
- Podemos agora definir os estados independentes:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x''$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x'$$

- E $|\Psi_1\rangle$ é, no fundo, uma sobreposição destes estados:

$$|\Psi_1\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

Visualização geométrica

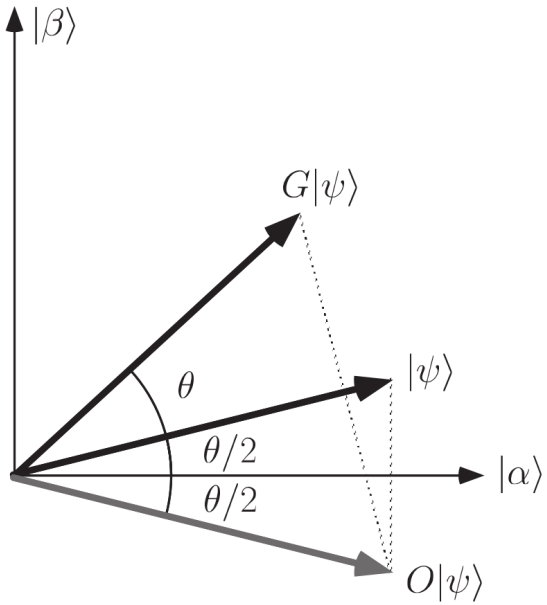
- Se nos lembrarmos o que fazia o oráculo, percebos que, nesta nova base, essa operação corresponde a uma refecção ao eixo $|\alpha\rangle$
- Menos intuitivamente, conseguimos perceber que o resto da iteração de grover corresponde a outra reflecção, mas relativamente ao nosso $|\Psi\rangle$ inicial.
- Duas reflecções são uma rotação.

Visualização geométrica

- Se nos lembrarmos o que fazia o oráculo, percebos que, nesta nova base, essa operação corresponde a uma refecção ao eixo $|\alpha\rangle$
- Menos intuitivamente, conseguimos perceber que o resto da iteração de grover corresponde a outra reflecção, mas relativamente ao nosso $|\Psi\rangle$ inicial.
- Duas reflecções são uma rotação.
- So what?

Visualização geométrica

- This is what:
- Com $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$ temos:
- $|\Psi\rangle = cos(\frac{\theta}{2})\,|\alpha\rangle + sen(\frac{\theta}{2})\,|\beta\rangle$
- $G\,|\Psi\rangle = cos(\frac{3\theta}{2})\,|\alpha\rangle + sen(\frac{3\theta}{2})\,|\beta\rangle$
- $G^k\,|\Psi\rangle = cos(\frac{2k+1}{2}\theta)\,|\alpha\rangle + sen(\frac{2k+1}{2}\theta)\,|\beta\rangle$



Índice

Recomeçando...
O que vos vamos falar.
Mas porquê?
Transformada de Fourier quântica
Motivação
RSA Cryptosystem
O Circuito
Fases
Algoritmos de procura quântica
O problema
O oráculo
Para RSA
O procedimento
A iteração de Grover
Visualização geométrica
Conclusões

CONCLUSÕES