# Computação Quântica: uma perspectiva de Computação Paralela

*William A. M. Gnann*

# Computação Quântica

- "É como probabilidade, mas com números complexos." - Aaronson, Scott.
- A ideia surgiu da dificuldade em simular sistemas quânticos usando computação tradicional.

# Propriedades

- **Sobreposição**;
- **Observação**;
- Interferência;
- Reversibilidade;
- Emaranhamento.

# Sobreposição

- Um sistema quântico pode assumir múltiplos estados probabilisticamente;
- Propriedade muito explorada para algoritmos quânticos;
- Talvez o coração do "paralelismo quântico".

# *qubit*

- Versão quântica dos nossos conhecidos *bits*;

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

# *qubits*

- Vetor sobre os números complexos;
- $\sum |a_i|^2 = 1$;
- Para *n qubits*, precisaremos de $2^n$ elementos.

$$q = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$$

# *bit* vs *qbit*

| ***bit*** | ***qbit*** |
|---|---|
| número | vetor |
| $n$ | $2^n$ |
| determinístico | probabilístico |

# Observação

- Colapsa, com probabilidade $|a_i|^2$, para o estado $|i\rangle$;
- Não é reversível.

# Como computar?

- As portas lógicas quânticas são transformações lineares;
- Sobreposição → Interferência → Observação.

# Transformações Lineares

- São unitárias: preservam a norma 2;
- Corolário: mantém uma distribuição de probabilidade sobre os *qubits*;
- São reversíveis.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Porta Hadamard

# Algoritmo Quântico

- Um algoritmo quântico é, essencialmente, uma sucessão de transformações sobre *qubits*;
- Objetivo: maximizar a probabilidade de observar o estado correto por meio de interferência.

# Algoritmo de Grover

"Encontra um determinado elemento num banco de dados em $O(\sqrt{n})$."

# Algoritmo de Grover

"Encontra um determinado elemento num banco de dados em $O(\sqrt{n})$."

# Algoritmo de Grover

"Encontra um determinado elemento num banco de dados em $O(\sqrt{n})$."!!1!1!

# Algoritmo de Grover

- Dada uma função $f : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$, encontrar o índice $i$ tal que $f(i) = k$.
- $f$ é dada por um **oráculo quântico**;
- Classicamente, no pior caso, precisamos inspecionar todos os elementos.

# Grover: ideia

- Inversão de fase: feita via oráculo;
- Reflexão pela média: feita por um conjunto de operadores;
- Usar ambas as inversões para maximizar a probabilidade de observar o *i* correto.

# Inversão de fase

- Exemplos de oráculo com 2 *qbits*:

$$\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

# Reflexão pela média

- Reflete todas as fases a partir da média.
- A transformação que faz a reflexão é:

$$2H|0\rangle\langle 0|H - I$$

$2H|O\rangle\langle O|H - I$


$$2H|O\rangle\langle O|H - I$$

# Difusão

A difusão de Grover consiste numa aplicação do oráculo, **U**, para inverter a fase e numa aplicação da reflexão, **R**.

# Algoritmo de Grover

GROVER($U(f)$)

inicializa $|q\rangle$ com $a_i = 1/\sqrt{n}$

para $i$ de $1$ até $\pi\sqrt{n}/4$

$|q\rangle \leftarrow U|q\rangle$

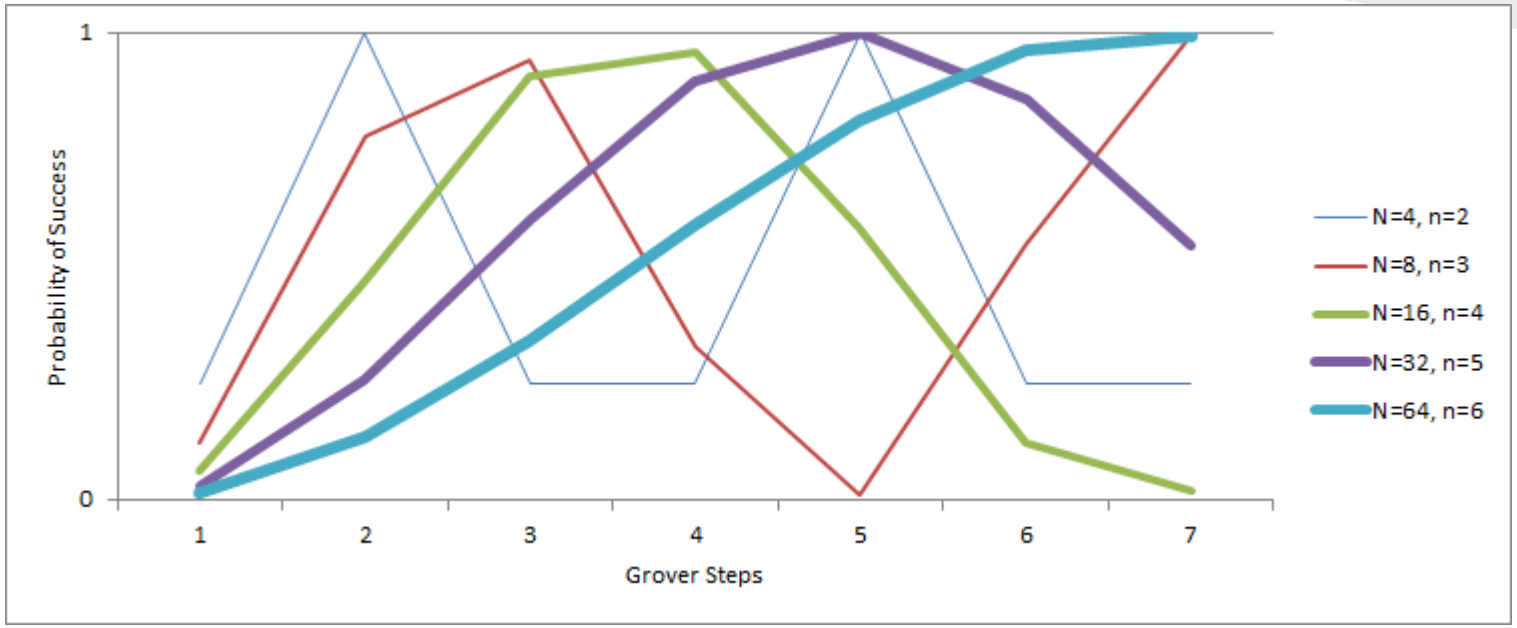
$|q\rangle \leftarrow R|q\rangle$

devolva observe($|q\rangle$)

# Consumo de tempo

- Para cada difusão, haverá um aumento de $\sqrt{2}/\sqrt{n}$ no na fase que desejamos;
- Em $\sqrt{n}/2$ passos chegamos em $1/\sqrt{2}$;
- Em $\pi\sqrt{n}/4$ passos atingimos o máximo;
- Passando disso, **piora**!

# Consumo de tempo




Fonte: http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm


$2H|O\rangle\langle O|H - I$