

# BUSCA EFICAZ E EFICIENTE EM UMA BASE DESORDENADA USANDO UM COMPUTADOR QUÂNTICO

Bruno V. T. Ferreira<sup>1</sup>, Roberto Baginski Batista Santos<sup>2</sup>

<sup>1</sup> Departamento de Engenharia Química, Centro Universitário FEI

<sup>2</sup> Departamento de Física, Centro Universitário FEI

bruno.v.t.ferreira@hotmail.com, rsantos@fei.edu.br

**Resumo:** Neste trabalho, avaliamos a eficácia das portas lógicas quânticas  $X$ ,  $Z$ ,  $H$  e  $cZ$  necessárias para a execução do algoritmo de Grover, separadamente, através do processador ibmqx2 da IBM. Com a alta eficácia obtida nestes testes, construímos e avaliamos a eficácia do algoritmo a fim de determinar sua eficiência ao realizar uma busca de determinado estado quântico em uma base desordenada. Apesar de apresentar disparidades nas probabilidades de sucesso na obtenção de cada estado, obtivemos elevada eficácia em todos os testes realizados.

## 1. Introdução

Na FEI, as listas de presença são ordenadas pelo número de matrícula dos alunos. Como um professor deve fazer para encontrar um aluno pelo nome?

Como os registros de nome são desordenados na lista de presença, o professor pode procurar aleatoriamente pela lista ou pode procurar sequencialmente pela lista de  $N$  nomes.

Em qualquer uma destas estratégias, o professor pode ter de consultar a lista  $N$  vezes até encontrar o nome pelo qual estava procurando. Este é o melhor resultado possível na computação clássica para buscas em bases desordenadas.

Na computação quântica, há uma estratégia melhor, que é usar o algoritmo de Grover, que permite encontrar o registro procurado em aproximadamente  $\pi\sqrt{N}/4$  consultas, o que corresponde a uma aceleração quadrática em relação ao melhor algoritmo clássico [1]. Assim, esta tarefa seria realizada mais eficientemente em um computador quântico do que em um computador clássico.

Em um computador quântico, os bits são substituídos por qubits (bits quânticos). Enquanto um bit pode estar apenas no estado 0 ou no estado 1, um qubit pode estar no estado [2]

$$|q\rangle = c_0|0\rangle + c_1|1\rangle \quad (1)$$

que é uma superposição dos estados  $|0\rangle$  e  $|1\rangle$ . Os coeficientes  $c_0$  e  $c_1$  são números complexos chamados amplitudes de probabilidade. Esta superposição é uma expressão da natureza ondulatória da matéria.

Se pensarmos na superposição como a soma das componentes  $|0\rangle$  e  $|1\rangle$ , os coeficientes  $c_0$  e  $c_1$  caracterizam as amplitudes destas componentes. A superposição só pode existir enquanto o qubit não é observado. Quando o qubit é observado, a probabilidade de obter o estado  $|0\rangle$  é  $|c_0|^2$  e a probabilidade de obter o estado  $|1\rangle$  é  $|c_1|^2$ . Quando há dois qubits, a superposição se torna

$$|q_1q_0\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle. \quad (2)$$

O algoritmo de Grover modifica as amplitudes da superposição produzindo um efeito de interferência entre

as componentes para aumentar a probabilidade de se encontrar o estado que corresponde ao item procurado, minimizando as demais probabilidades.

A modificação das amplitudes é feita com a aplicação de portas quânticas aos qubits. A porta  $X$  faz a troca  $|0\rangle \Leftrightarrow |1\rangle$  e é a generalização quântica da porta lógica NOT. A ação da porta  $Z$  é de trocar o sinal do coeficiente da componente  $|1\rangle$  do qubit e não possui análogo clássico. A porta  $H$  cria as superposições balanceadas

$$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \quad (3)$$

a partir dos estados  $|0\rangle$  e  $|1\rangle$ , respectivamente. A porta  $cZ$  é uma porta de dois qubits, isto é, sua ação sobre o qubit alvo depende do estado de outro qubit, o qubit de controle. Se o qubit de controle estiver no estado  $|1\rangle$ , a porta  $Z$  é aplicada ao qubit alvo, trocando o sinal do coeficiente da componente  $|1\rangle$ ; se o qubit de controle estiver no estado  $|0\rangle$ , o qubit alvo permanece inalterado.

Neste trabalho, vamos determinar a eficácia com que o computador quântico ibmqx2 da IBM é capaz de usar estas portas quânticas para encontrar um registro em uma base desordenada de quatro elementos de modo eficiente, com apenas uma única consulta.

## 2. Metodologia

O algoritmo de Grover consiste em uma sequência de etapas, como mostra a figura 1.

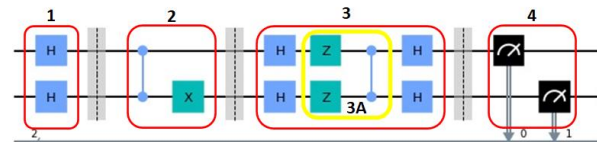


Figura 1. Circuito quântico para encontrar o item  $|01\rangle$ .

Na etapa 1, os qubits, que são inicializados sempre no estado  $|0\rangle$ , são colocados em superposições balanceadas pelo uso da porta  $H$  em cada qubit.

Na etapa 2, é feita uma consulta a um oráculo quântico capaz de identificar o item procurado. No caso mostrado na figura, o oráculo está identificando o item associado ao estado  $|01\rangle$ . O efeito do oráculo é marcar o estado procurado trocando o sinal do coeficiente que corresponde a ele no meio da superposição criada na etapa 1. Isso é feito pelo uso das portas  $cZ$  e  $X$ . Apenas o oráculo é modificado para cada item.

Na etapa 3, atua o operador de Grover para amplificação de amplitude. O núcleo desta etapa são as portas quânticas da etapa 3A, em que ocorre a inversão em torno da média ilustrada na figura 2. O resultado da etapa 3 é aumentar a amplitude da componente procurada ao mesmo tempo em que as amplitudes das demais componentes são reduzidas.

Este efeito de interferência quântica aumenta a probabilidade de que o estado procurado seja observado na etapa 4, em que todos qubits são medidos. Como se trata de um processamento probabilístico, não há garantia que o estado procurado será observado todas as vezes. Porém, a repetição das etapas 2 e 3 faz a probabilidade de sucesso se aproximar cada vez mais de 100%. Cada repetição das etapas 2 e 3 equivale a uma nova consulta à lista de itens.

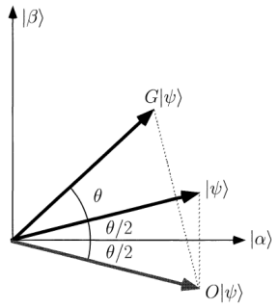


Figura 1. Inversão em torno da média. Fonte: ref [2].

A medida de eficácia escolhida foi a fidelidade

$$\mathcal{F} = \sum_i \sqrt{p_i \tilde{p}_i} \quad (4)$$

que é uma medida da semelhança entre duas distribuições de probabilidade. Na equação (4),  $p_i$  e  $\tilde{p}_i$  são a probabilidade observada experimentalmente e a probabilidade esperada com base na análise teórica do algoritmo. Se a fidelidade é alta, isso significa que a distribuição experimental de probabilidades é semelhante ao esperado e o computador quântico é eficaz, isto é, reproduz bem o que a análise teórica previa. Se a fidelidade é baixa, o computador quântico não é eficaz.

Inicialmente, foram testadas as portas  $X$ ,  $H$ ,  $Z$  e  $cZ$ , que são as portas usadas no algoritmo de Grover. Cada teste foi realizado 1024 vezes, o que permite obter probabilidades com incerteza em torno de 0,1%.

Em seguida o algoritmo de Grover foi executado 1024 vezes para cada um dos quatro registros possíveis com dois bits: 00, 01, 10 e 11.

Todos os testes foram realizados no computador quântico *ibmqx2* da IBM, cujo acesso é feito por um serviço em nuvem [3]. O *ibmqx2* é composto por cinco qubits transmonicos. Cada *transmon* é uma junção Josephson supercondutora ligada a um capacitor de grande capacitância. Esta configuração é equivalente a um sistema de dois níveis  $|0\rangle$  e  $|1\rangle$  com estados de energia bem definidas e redução dos efeitos da flutuação de carga na junção.

### 3. Resultados

A menor fidelidade observada nos testes para as portas  $X$ ,  $H$ ,  $Z$  e  $cZ$  foi de 0,97. Isso significa que o computador quântico usado é eficaz ao executar as portas quânticas usadas no algoritmo de Grover.

A tabela 1 mostra a probabilidade de sucesso e a fidelidade para os testes experimentais para busca em uma base desordenada de quatro itens usando, em cada caso, 1024 execuções do algoritmo de Grover. Em todos

os casos, a etapa 2 do algoritmo foi realizada uma única vez, isto é, houve apenas uma consulta.

Tabela 1. Resultados experimentais para busca em base desordenada de quatro itens usando o algoritmo de Grover com uma única consulta.

Estado procurado	Probabilidade de sucesso	Fidelidade
$ 00\rangle$	89,0%	0,943
$ 01\rangle$	77,4%	0,880
$ 10\rangle$	63,9%	0,799
$ 11\rangle$	83,9%	0,915

Fonte: autores.

Os resultados mostram que, na melhor situação, houve quase 90% de chance de encontrar o item procurado usando o algoritmo de Grover com apenas uma consulta. No pior caso, o item procurado ainda foi encontrado mais de 60% das vezes.

Para comparação, probabilidade de encontrar o item procurado com apenas uma consulta seria de apenas 25% na computação clássica, bem menor do que a obtida usando a amplificação de amplitude permitida pela interferência quântica. Não está claro o que leva alguns dos estados serem encontrados com taxa de sucesso bem menor do que outros.

### 4. Conclusões

Fizemos uma avaliação da eficácia do computador quântico *ibmqx2* da IBM ao executar as portas  $X$ ,  $Z$ ,  $H$  e  $cZ$  e ao executar o algoritmo de Grover para buscas em bases desordenadas. As portas quânticas foram executadas com alta fidelidade, o que é uma condição necessária para que um algoritmo quântico possa ser executado com eficácia. Ainda que a base usada tenha sido pequena, contendo apenas quatro itens, os resultados mostraram que o computador quântico foi capaz de encontrar o item procurado com probabilidade superior a 60% com uma única consulta, o que é mais do que o dobro do resultado que seria obtido na computação clássica com uma única consulta.

### 5. Referências

- [1] GROVER, L. A fast quantum mechanical algorithm for database search. In: ACM Symposium on Theory of Computing, 28. **Proceedings...** p.212–219, 1996.
- [2] NIELSEN, M.A.; CHUANG, I.L. **Quantum Computation and Quantum Information**. Cambridge: Cambridge University Press, 2000.
- [3] IBM. **IBM Quantum Experience**. Disponível em <<https://quantum-computing.ibm.com>>. Acesso em: 25 set. 2020.

### Agradecimentos

Ao Centro Universitário FEI pela concessão da bolsa de iniciação científica e à IBM pelo uso do computador quântico *ibmqx2*.

<sup>1</sup> Aluno de IC do Centro Universitário FEI. Projeto com vigência de 12/19 a 11/20