Quantum Oracles - Como transformar problemas clássicos em quânticos

Alexandre Silva,
Ciências da Computação

UNIVEM

Maurício Duarte (Mestre)

Marília, outubro de 2023.

OBJETIVO

- *Computação quântica é, teoricamente, limitada à certas áreas;*
- *Como aplicar a computação quântica em mais áreas de forma efetiva (quantum oracles).*

METODOLOGIA

- *Elencagem dos tipos conhecidos de quantum oracles;*
- *Pesquisa de problemas já resolvidos e suas estratégias;*
- *Enumeração de problemas diversos ainda não resolvidos: exemplos de problemas: comparação de preços de produtos, encoding de dados de games, etc.;*
- *Implementação dos circuitos;*
- *Testes usando simuladores e máquinas reais;*
- *Apresentação dos resultados em comparação à algoritmos clássicos.*

DESENVOLVIMENTO

O que é um oracle?

- Classicamente representa uma máquina de turing que implementa uma função com O(1) (função ideal);
- dados internos ficam escondidos para a redução de complexidade do estudo;
- Usada para estudos de complexidade;
- Quantum oracles tomam proveito dos efeitos quânticos;
- Usado pela maior parte dos algoritmos quânticos;
- Ajudaram a apresentar um avanço perante algoritmos clássicos.

DESENVOLVIMENTO

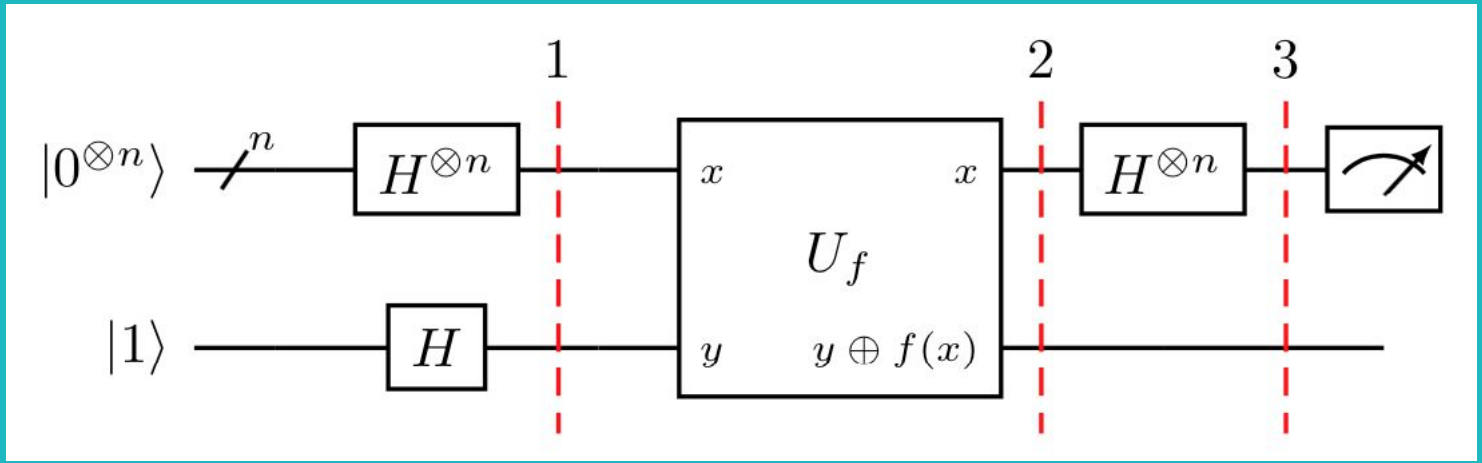
Tipos de Oracles

DESENVOLVIMENTO

Boolean Oracle

- Aplica uma função booleana à entrada e/ou representa a saída como um valor booleano;
- Manipula uma bit string e retorna outra bit string;
- Usado em algoritmos como o de Deutsch Jozsa.

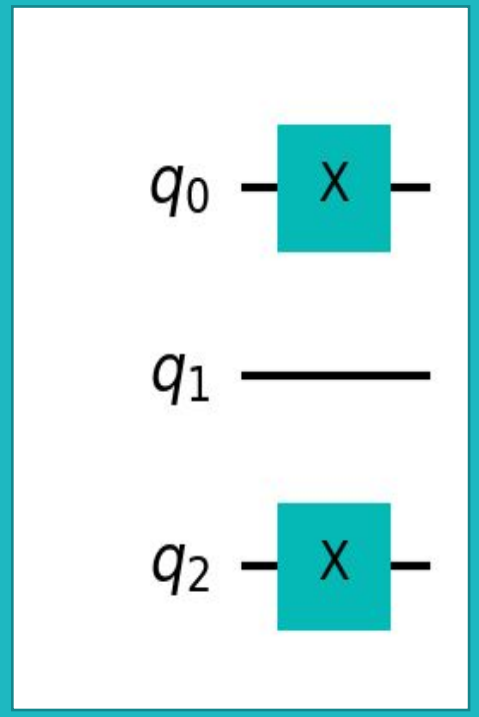
Algoritmo de Deutsch Jozsa



fonte: Qiskit (IBM)

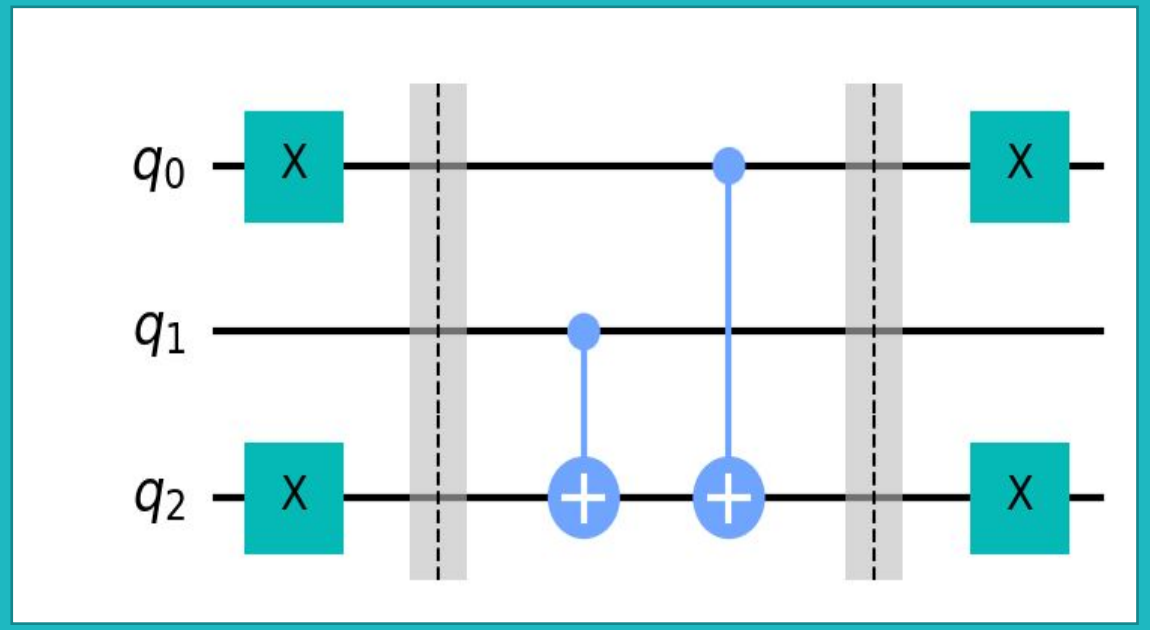
DESENVOLVIMENTO

oracle constante



fonte: criação própria

oracle balanceado



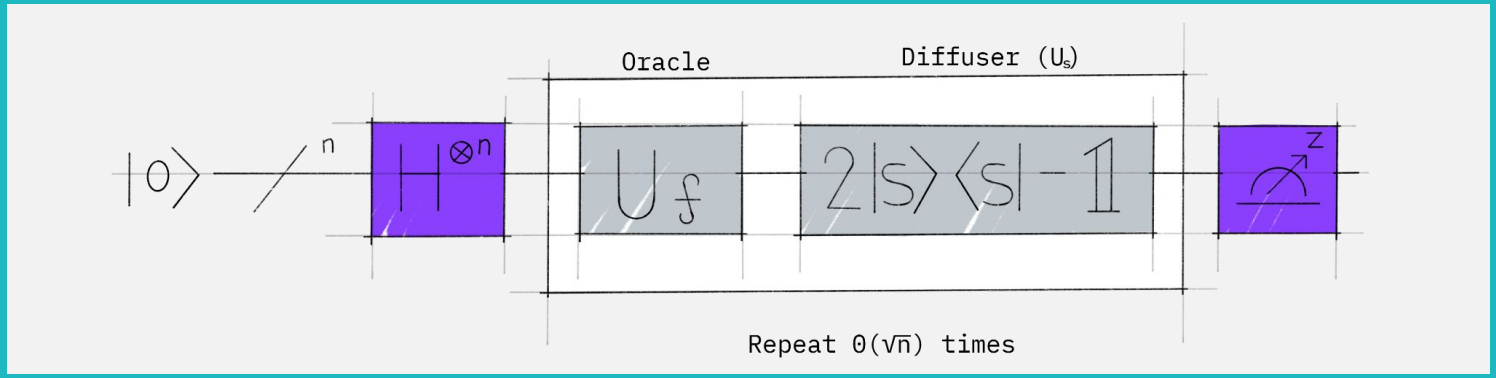
fonte: criação própria

DESENVOLVIMENTO

Phase Oracle

- Aplica uma fase em determinados valores;
- Usado para marcar valores esperados;
- Usado em algoritmos como o de Bernstein-Vazirani e de Grover.

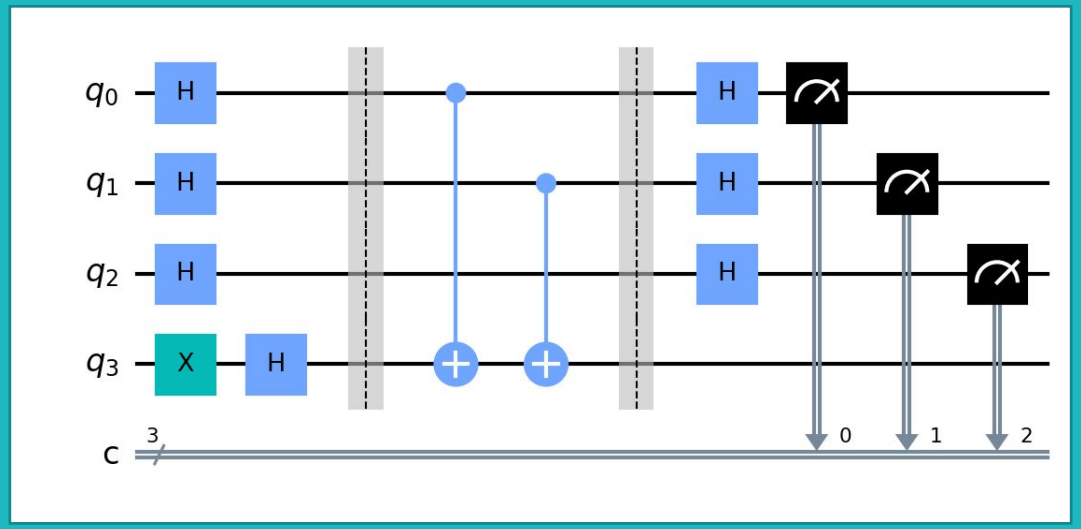
Algoritmo de Grover



fonte: Qiskit (IBM)

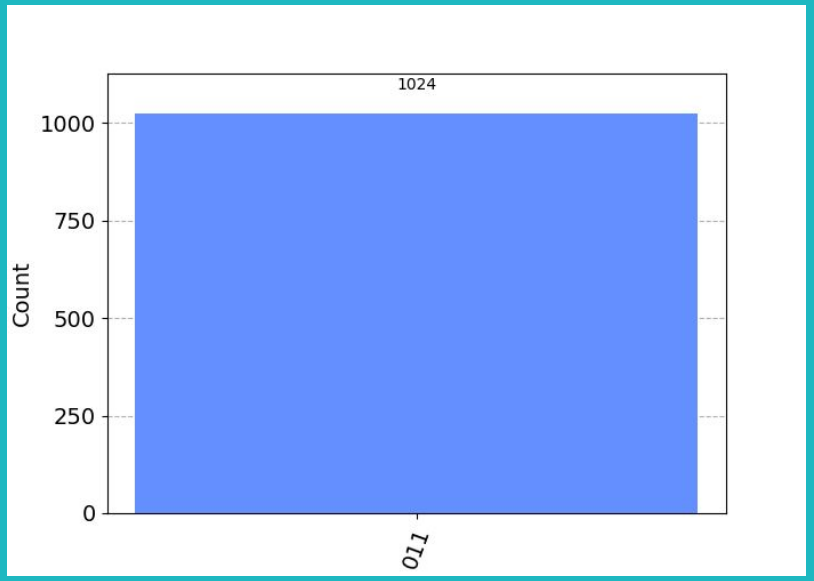
DESENVOLVIMENTO

Phase oracle (phase kickback)



fonte: criação própria

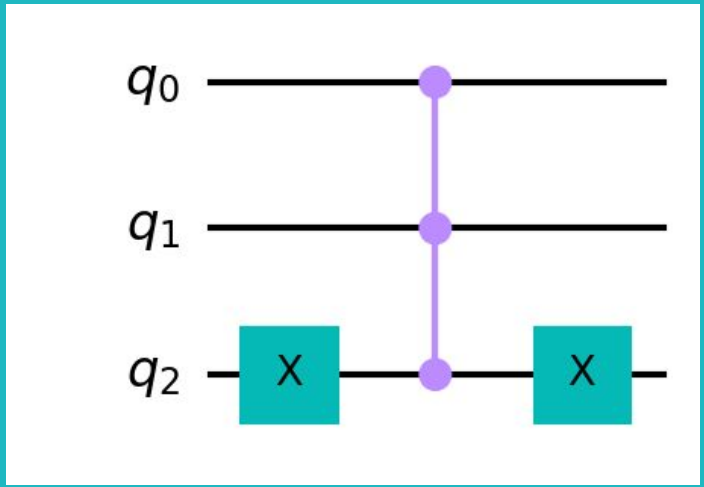
resultados



fonte: criação própria

DESENVOLVIMENTO

Phase oracle (ccz)



fonte: criação própria

unitary

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

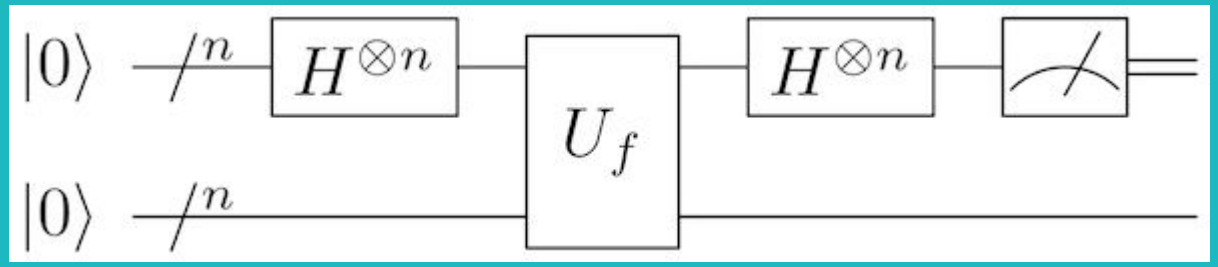
fonte: criação própria

DESENVOLVIMENTO

Simon's Oracle

- Também é um oracle booleano;
- Encontra períodos entre bitstrings;
- Usado pelo algoritmo de Simon e é a base para o algoritmo de Shor.

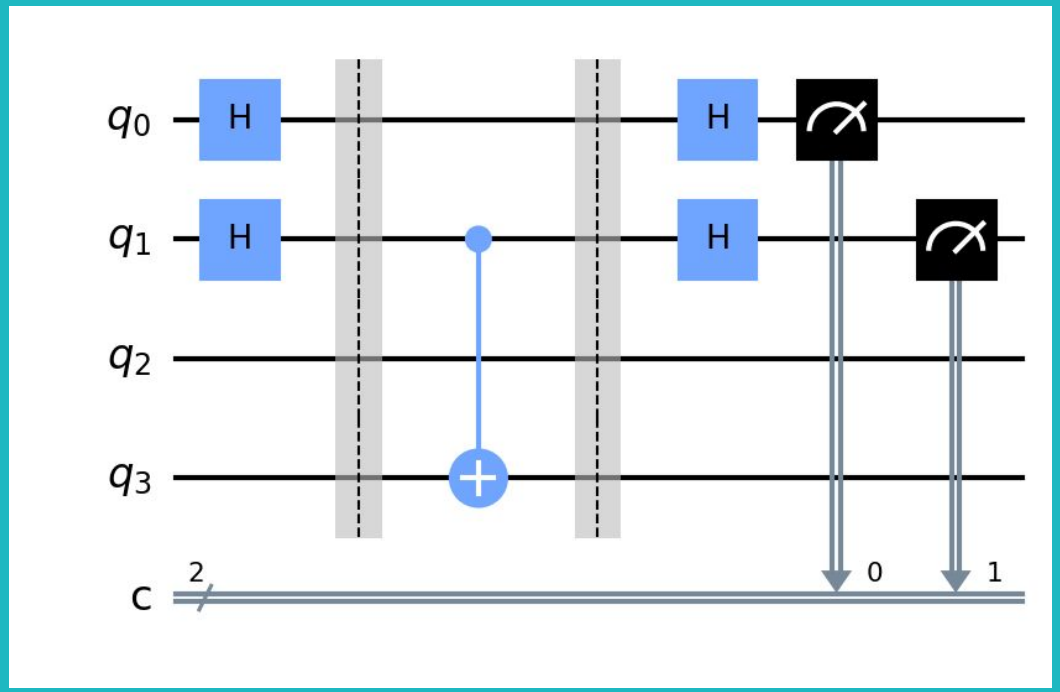
Algoritmo de Simon



fonte: AWS(Amazon)

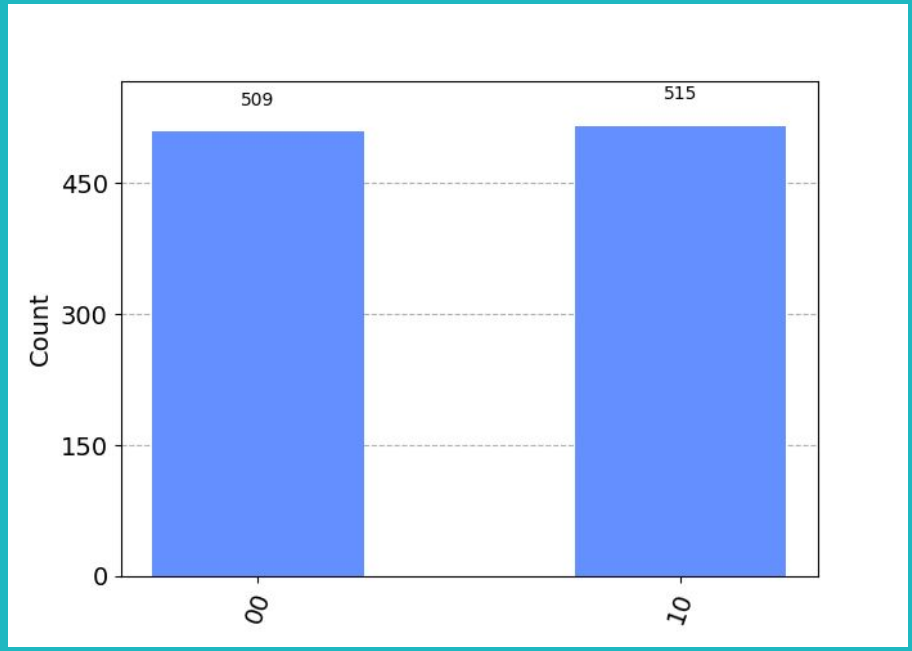
DESENVOLVIMENTO

Implementação



fonte: criação própria

resultados



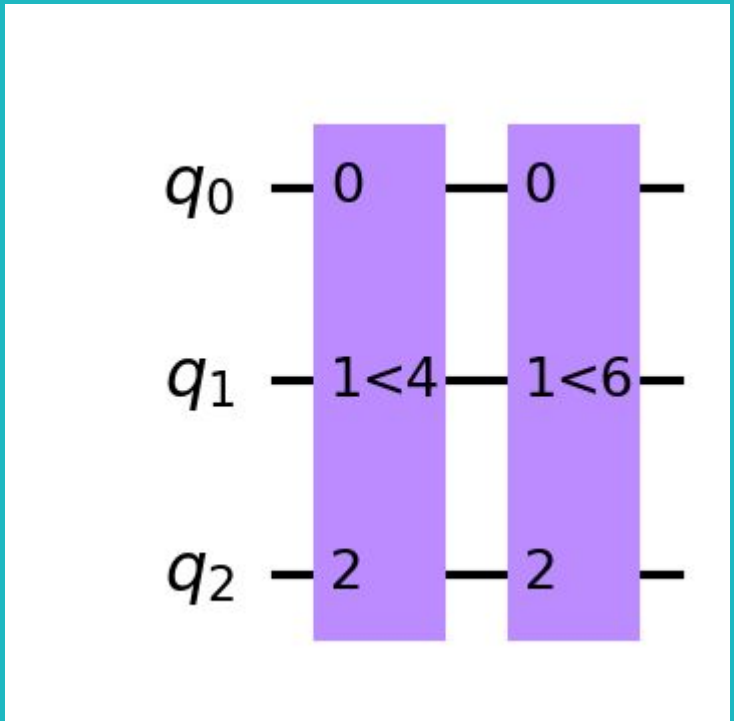
fonte: criação própria

DESENVOLVIMENTO

Circuitos úteis

DESENVOLVIMENTO

valores intermediários



fonte: criação própria

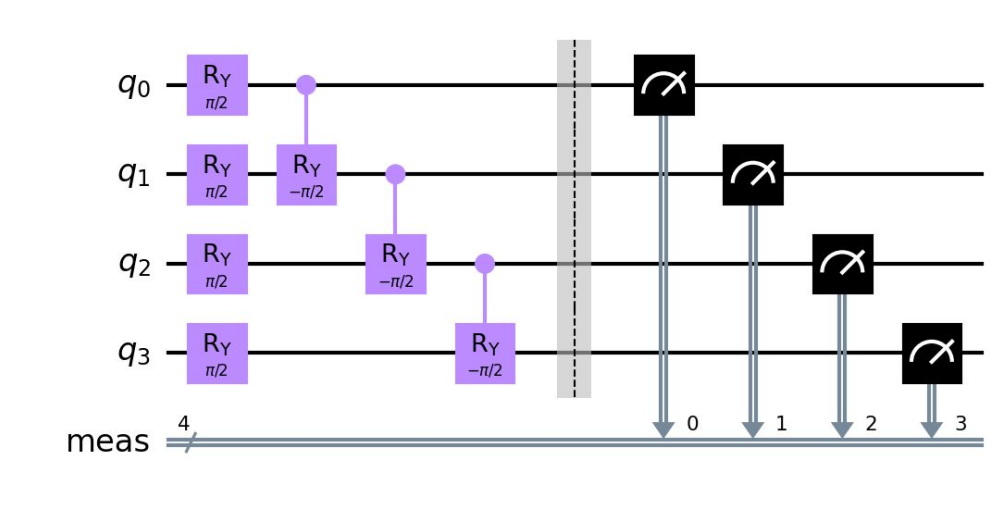
unitary

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

fonte: criação própria

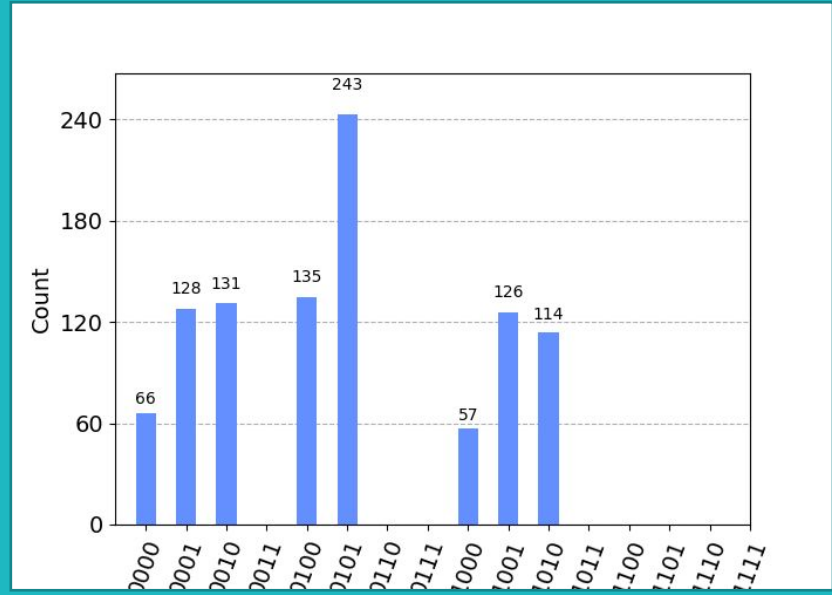
DESENVOLVIMENTO

Fibonacci



fonte: criação própria

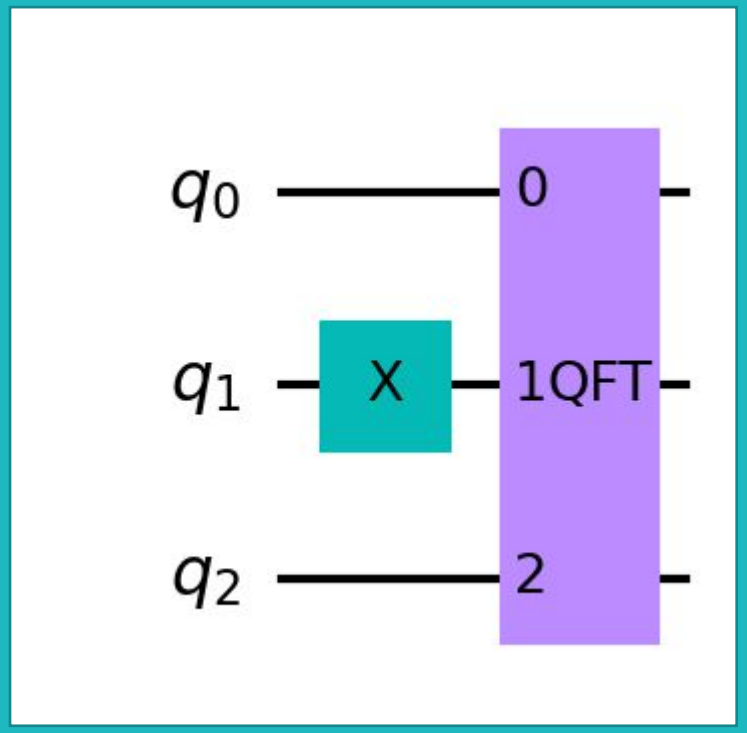
Medições



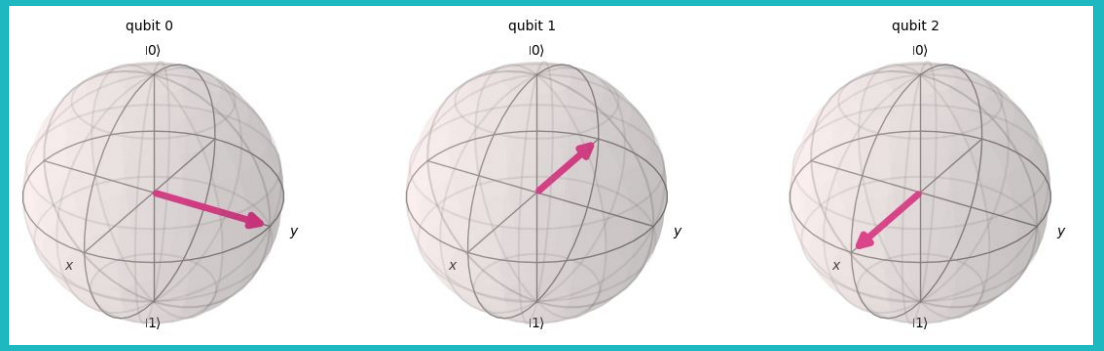
fonte: criação própria

DESENVOLVIMENTO

QFT



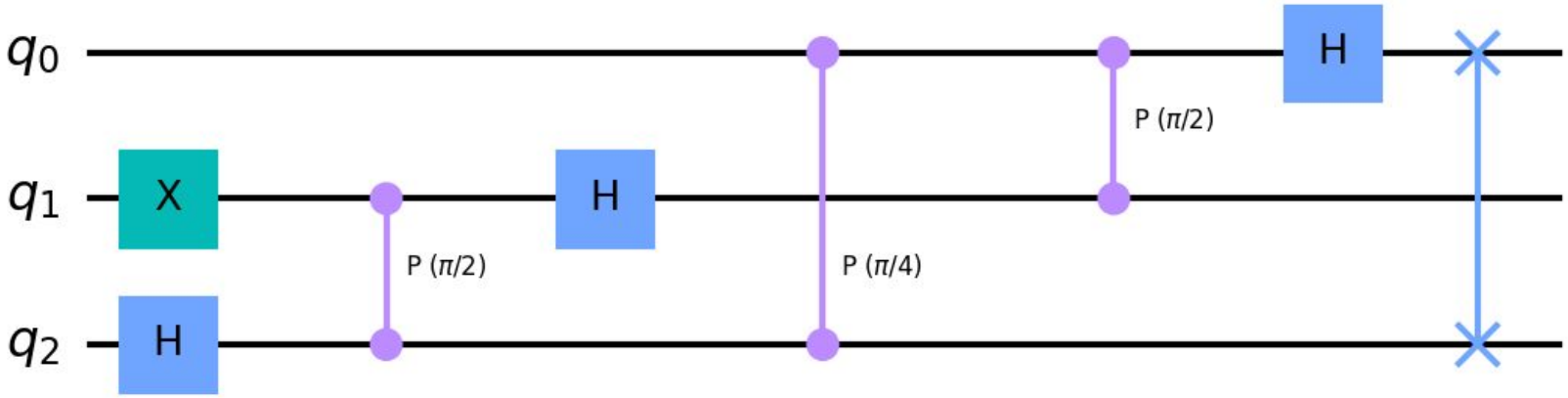
fonte: criação própria



fonte: criação própria

DESENVOLVIMENTO

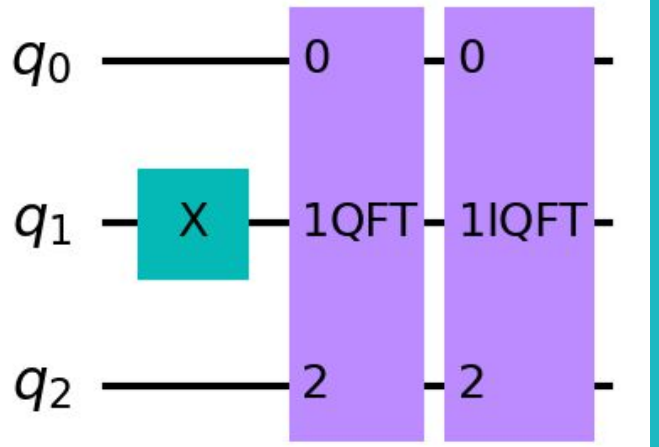
QFT

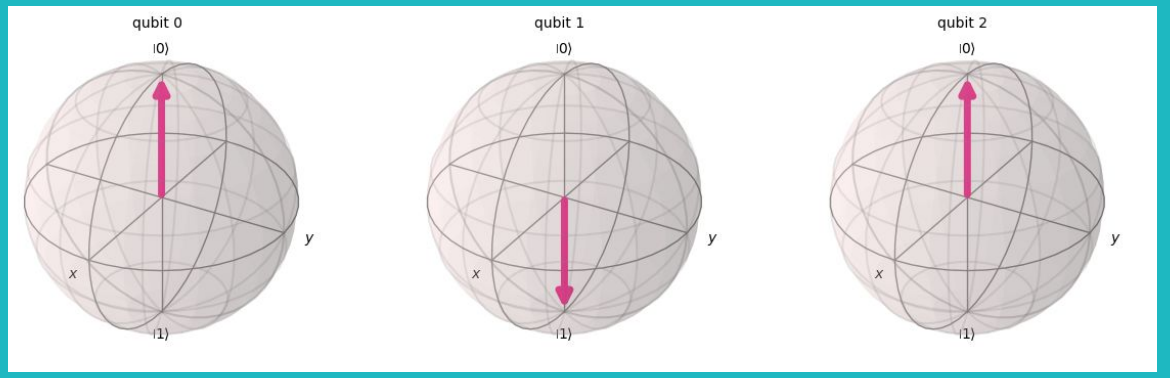


fonte: criação própria

DESENVOLVIMENTO

QFT†

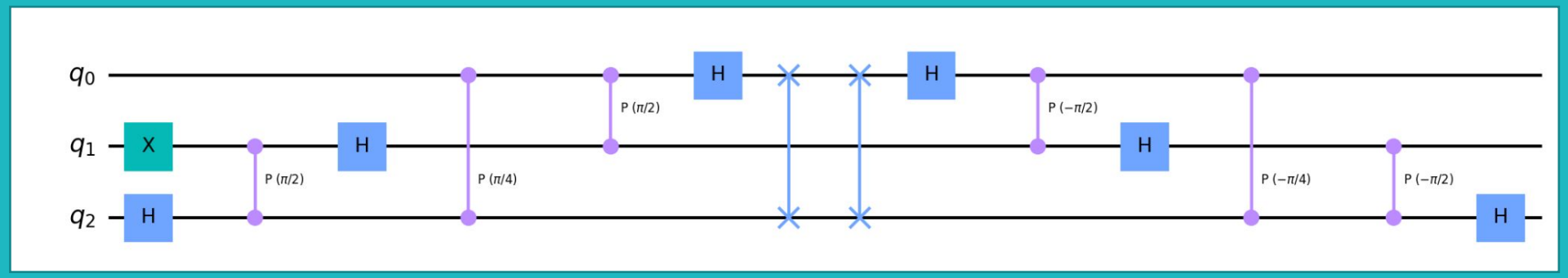




fonte: criação própria

DESENVOLVIMENTO

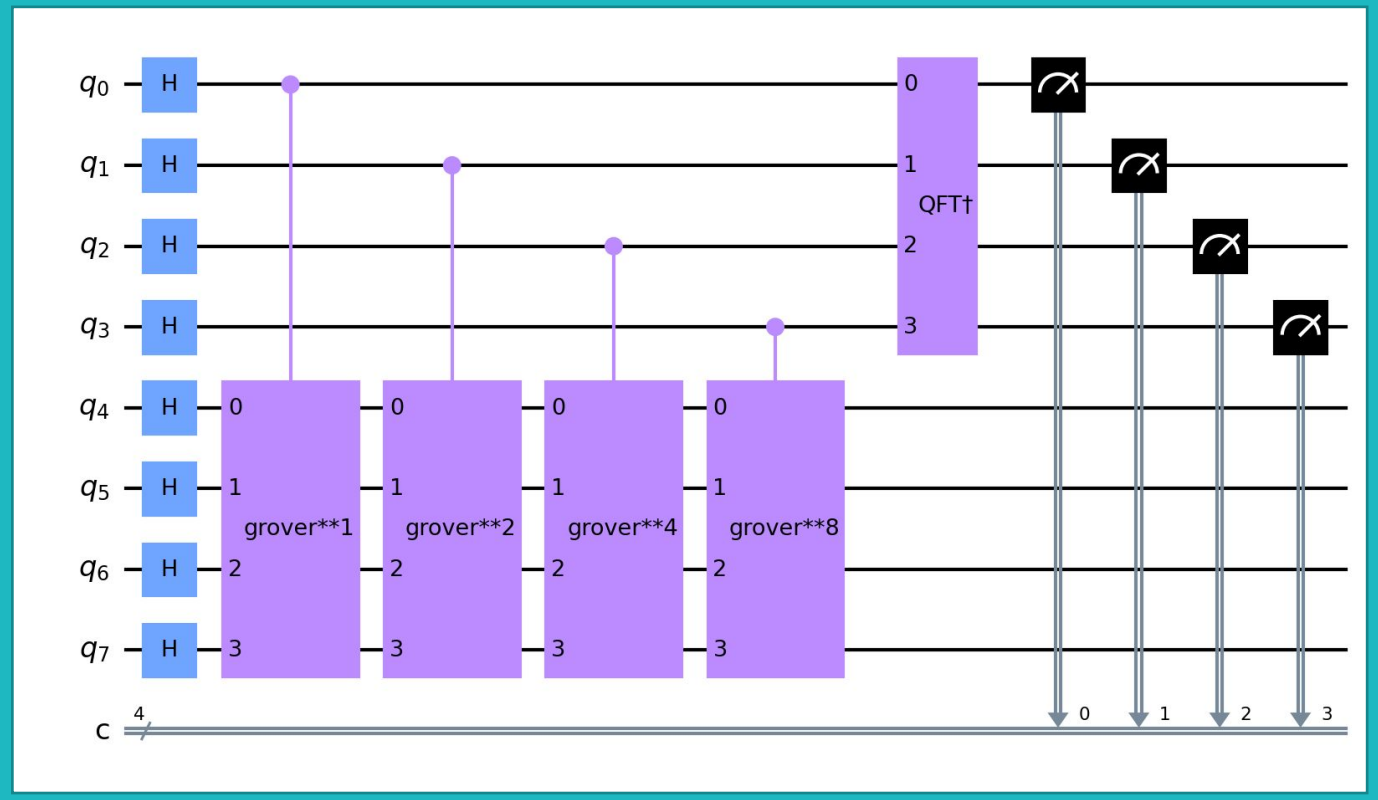
QFT†



fonte: criação própria

DESENVOLVIMENTO

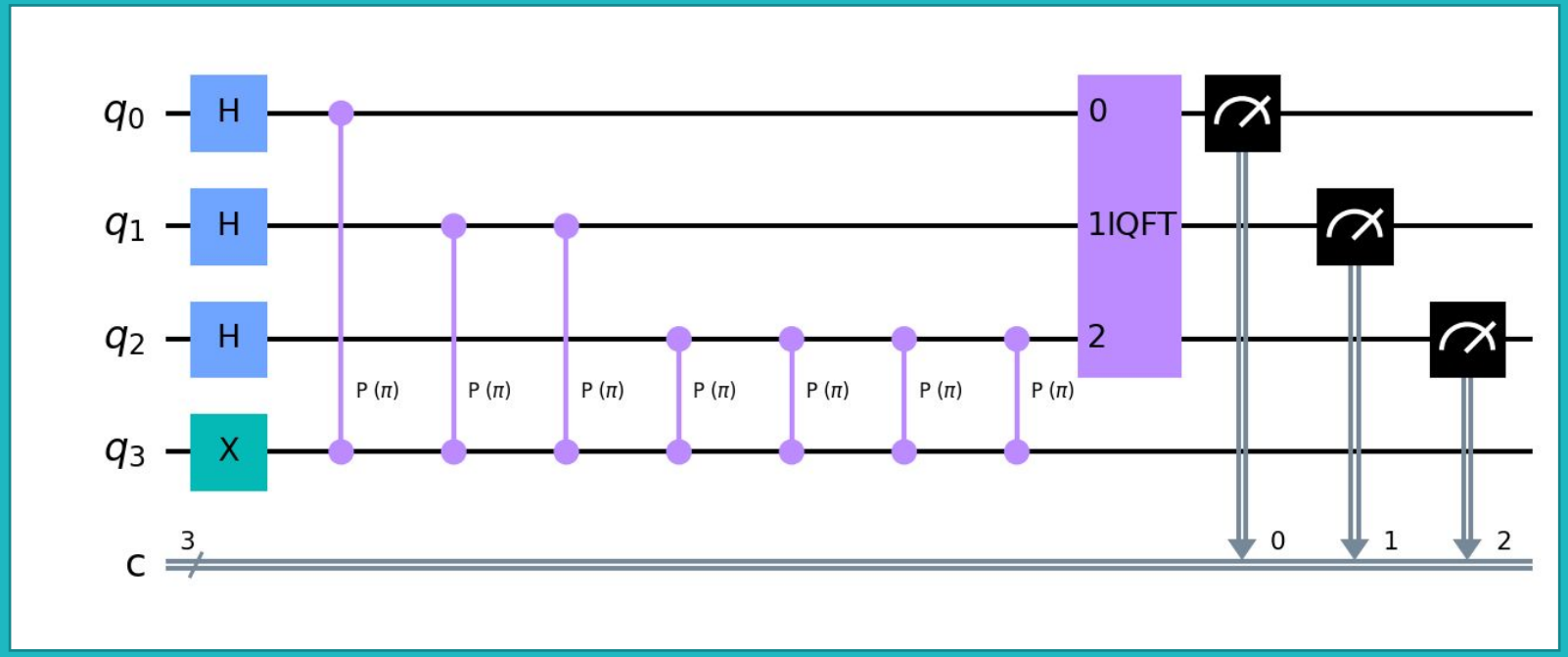
Quantum Counting



fonte: criação própria

DESENVOLVIMENTO

QPE



fonte: criação própria

CONSIDERAÇÕES FINAIS

- Phase Oracle/Grover's Algorithm são os mais úteis para esses casos (ESPERADO);
- Quantidade necessária de medições pode ser um empecilho (PARCIAL);
- Pós-Processamento pode ser um ponto chave para resultados melhores (PARCIAL);
- Classificar problemas atuais em problemas quânticos já resolvidos pode ser o melhor approach (PARCIAL);
- QPE é uma ferramenta poderosa para extração de informações dos dados (um auxiliar aos quantum oracles) (PARCIAL).

CONSIDERAÇÕES FINAIS

Approach	Algoritmo
Busca	Grover
Períodos	Simon
Booleanos	Deutsch-Jozsa/Bernstein-Vazirani
Contagem	Quantum Counting
Encoding	QFT
Extração	QPE

Quantum Oracles - Como transformar problemas clássicos em quânticos

Alexandre Silva

Centro Universitário Eurípides de Marília - UNIVEM

alexandresilvaunivem@gmail.com

Out/2023

BIBLIOGRAFIA

O'DONNELL, R. Lecture 5: Quantum Query Complexity. [s.l: s.n.]. Disponível em: <https://www.cs.cmu.edu/~odonnell/quantum15/lecture05.pdf>. Acesso em: 4 set. 2023.

O'DONNELL, R. Lecture 13: Lower Bounds using the Adversary Method. [s.l: s.n.]. Disponível em: <https://www.cs.cmu.edu/~odonnell/quantum15/lecture13.pdf>. Acesso em: 5 set. 2023.

SOARE, R. I. Turing oracle machines, online computing, and three displacements in computability theory. Annals of Pure and Applied Logic, v. 160, n. 3, p. 368–399, set. 2009.

BRODKORB, L.; EPSTEIN, R. The Entscheidungsproblem and Alan Turing. [s.l: s.n.]. Disponível em: <https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/brodkorb.pdf>. Acesso em: 7 set. 2023.

AMREEN, S.; HOQUE, R. Oracle Turing Machines. [s.l: s.n.]. Disponível em: <https://web.eecs.utk.edu/~bmaclenn/Classes/494-594-UC-F15/presentations/OTM.pdf>. Acesso em: 9 set. 2023.

KALYANASUNDARAM, S. mod04lec23 - Oracle Turing Machines. Disponível em: <https://www.youtube.com/watch?v=ElSExH4Xolc>. Acesso em: 12 set. 2023.

DAVIS, M. Turing Reducibility? [s.l: s.n.]. Disponível em: <https://www.ams.org/notices/200610/whatis-davis.pdf>. Acesso em: 12 set. 2023.

SIPSER, M. Reductions 1.1 Introduction Reductions. [s.l: s.n.]. Disponível em: <https://courses.grainger.illinois.edu/cs373/fa2013/Lectures/lec23.pdf>. Acesso em: 14 set. 2023.

BIBLIOGRAFIA

What does it mean to be Turing reducible? Disponível em: <https://cs.stackexchange.com/questions/54576/what-does-it-mean-to-be-turing-reducible>. Acesso em: 15 set. 2023.

KOTHARI, R. An optimal quantum algorithm for the oracle identification problem. arXiv (Cornell University), 29 nov. 2013.

FAN, Y. A Generalization of the Deutsch-Jozsa Algorithm to Multi-Valued Quantum Logic. Disponível em: <https://arxiv.org/abs/0809.0932>. Acesso em: 20 set. 2023.

SUNDARAPPAN, K. How to build oracles for Quantum Algorithms. Disponível em: <https://www.youtube.com/watch?v=R0LYfPMElJg>. Acesso em: 24 set. 2023.

YAMAKAWA, T.; ZHANDRY, M. Classical vs Quantum Random Oracles. Disponível em: <https://eprint.iacr.org/2020/1270>. Acesso em: 27 set. 2023.

BACON, D. CSE 599d -Quantum Computing Simon's Algorithm. [s.l: s.n.]. Disponível em: <https://courses.cs.washington.edu/courses/cse599d/06wi/lecturenotes8.pdf>. Acesso em: 29 set. 2023.

BUHRMAN, H.; CLEVE, R.; WIGDERSON, A. Quantum vs. Classical Communication and Computation. arXiv (Cornell University), 14 fev. 1998.

SANCHEZ-RIVERO, J. et al. Some Initial Guidelines for Building Reusable Quantum Oracles. arXiv (Cornell University), 27 mar. 2023.

GILLIAM, A.; PISTOIA, M.; GONCIULEA, C. Canonical Construction of Quantum Oracles. arXiv (Cornell University), 18 jun. 2020.

BIBLIOGRAFIA

JOHANSSON, N.; LARSSON, J.-Å. Quantum Simulation Logic, Oracles, and the Quantum Advantage. Entropy, v. 21, n. 8, p. 800, 15 ago. 2019.

O.D. PRIMQULOV. The role of quantum algorithms in the solution of important problems. Zenodo (CERN European Organization for Nuclear Research), v. 2, n. 1, 31 ago. 2022.

WONG, T. G. Introduction to classical and quantum computing. Omaha: Rooted Groove. Copyright, 2022.

KANG, H. Quantum Phase Estimation. Disponível em: <https://learn.qiskit.org/course/ch-algorithms/quantum-phase-estimation>.

Quantum Fourier Transform. Disponível em: <https://learn.qiskit.org/course/ch-algorithms/quantum-fourier-transform>.