**PRÉ-PROJETO DE INICIAÇÃO CIENTÍFICA**

**Título: Quantum Oracles - Como transformar problemas clássicos em quânticos**

1. **Introdução**:

Computação quântica tem se tornado um dos principais interesse de *big techs* e governos que querem entender e manipular, da melhor forma possível, o “mundo quântico”. Com a iminência de algoritmos, como o de [Peter Shor](https://arxiv.org/pdf/quant-ph/9508027.pdf), que, teoricamente, ameaçam a privacidade e a segurança de transações online. A corrida se voltou para os estudos de *quantum hardware* e *software*.

Por serem máquinas complexas, das quais, precisam interagir e medir spins, ou outras propriedades, de átomos, elétrons, fótons e entre outros, é complexo descrever algoritmos que sejam confiáveis e que tenham algum benefício perante os clássicos. Devido a isso, computadores quânticos são limitados a certas áreas, como: química, física, matemática, economia e certas áreas das ciências da computação, como em criptografia, banco de dados e *machine learning*. Essas, conseguem tirar proveito de efeitos quânticos, como os de superposição e interferência, fazendo com que a computação quântica se sobreponha à clássica. Como exemplo, poderíamos utilizar o algoritmo de [Grover](https://arxiv.org/pdf/quant-ph/9605043.pdf) e aproveitar da superposição de estados para fazer pesquisas em bancos de dados desordenados com , onde é a quantidade de dados.

Contudo, nos principais algoritmos dessas áreas, há uma peça chave que pode ser o passo para implementar algoritmos mais abrangentes e úteis. Os *Quantum Oracles* são algoritmos extremamente versáteis, suas funções vão desde reconhecer funções constantes ou funções balanceadas, como no algoritmo de [*Deutsch*](https://www.daviddeutsch.org.uk/)*-*[*Jozsa*](https://www.damtp.cam.ac.uk/person/rj310), até aplicações em criptografia quântica, como no caso dos random oracles, assim mostrado por [Mihir Bellare](https://dl.acm.org/profile/81100585242) e [Phillip Rogaway](https://dl.acm.org/profile/81100228044). Além de serem amplamente usados para medir a eficiência e reduzir a complexidade de circuitos. Devido ao fato de conseguirmos abstrair uma função complexa para dentro de uma “caixa preta”, é possível não só tomar proveito de efeitos quânticos, como também facilitar cálculos e a compreensão de certos algoritmos, limitando o foco para apenas os resultados obtidos.

1. **Problema:**

A computação quântica está extremamente limitada hoje, não existem muitos casos reais aplicados no dia-a-dia. Isso pois, peças caras e complexas como essas, não podem ser “desperdiçadas” com “partes irrelevantes”.

Contudo, há a possibilidade de reciclar os quantum oracles de problemas mais complexos, como os mostrado anteriormente, e remodelá-los para problemas menores.

Assim como demonstrado por [Paul Nation](https://quantum-enablement.org/explore/author/paul-nation.html#) em um [post](https://quantum-enablement.org/posts/2023/2023-07-05-Finding_Waldo_with_Grover_Search.html) no site [Quantum Enablement](https://quantum-enablement.org/index.html) da IBM, seria possível reutilizar o algoritmo de Grover mapeando seu oracle para jogar o, irreverente, *Where's Waldo?*. Mesmo sendo um exemplo simples, isso abre brechas para o que mais poderíamos fazer.

Sendo assim, a questão é, até onde os *oracles* podem nos ajudar no dia-a-dia? e, como de fato aplicá-los à problemas mundanos?

1. **Hipótese:**

Como hipótese, poderíamos pensar, de maneira arbitrária, que problemas corriqueiros se limitam a perguntas e respostas. Sendo assim, poderíamos fazer o *encode* de um problema em um *phase oracle*, e baseado nas regras ali dentro contidas, podemos fazer consultas à ele e, assim como em brincadeiras de “quem sou eu”, como resposta ele devolve SIM ou NÃO.

1. **Objetivo Geral:**

Observando a possibilidade de testar múltiplas alternativas ao mesmo tempo, devido a superposição, que um quantum oracle oferece, usá-los em certas situações pode ser um fato vantajoso para as pessoas.

Sendo assim, essa pesquisa tem como objetivo primário encontrar como encontrar soluções quânticas, para resolver problemas diários. Visando abranger desde pesquisa de preços de produtos, até *encoding* de dados em *machine learning*.

1. **Objetivos Específicos:**

Além de objetivos de caráter técnico, visando a solução de problemas. Criar um artigo científico sobre tal tema, pode encorajar pessoas a aprenderem mais sobre o assunto e difundirem tais técnicas, resultando em um arsenal maior de recursos disponíveis para futuros pesquisadores da área.

1. **Justificativa**:

Como já demonstrado, algoritmos quânticos são um passo para o futuro das ciências. A pesquisa em Quantum oracles contribuirá para a abrangência do tema, com mais pessoas interessadas nesse tipo de ferramenta, será possível encontrar e resolver outros problemas, além de impor, empiricamente, novas maneiras mais otimizadas de implementação.

1. **Metodologia**

Para tal trabalho, será usado de métodos qualitativos, se baseando na seguinte estrutura:

1. Elencagem dos tipos conhecidos de *quantum oracles*;
2. Pesquisa de problemas já resolvidos e suas estratégias;
3. Enumeração de problemas diversos ainda não resolvidos: exemplos de problemas: comparação de preços de produtos, encoding de dados de games, etc. (mínimo 5);
4. Implementação dos circuitos;
5. Testes usando simuladores e máquinas reais;
6. Apresentação dos resultados em comparação à algoritmos clássicos.
7. **Cronograma**

| **Atividades** | **Ago.** | **Set.** | **Out.** | **Nov.** | **Dez.** | **Jan.** | **Fev.** | **Mar.** | **Abr.** | **Mai.** | **Jun.** | **Jul.** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Elaboração do projeto. | **x** |  |  |  |  |  |  |  |  |  |  |  |
| Revisão da Literatura |  | **x** | **x** |  |  |  |  |  |  |  |  |  |
| Fichamentos |  |  |  | **x** | **x** |  |  |  |  |  |  |  |
| Desenvolvimento da proposta |  |  |  |  |  | **x** | **x** | **x** |  |  |  |  |
| Redação Preliminar |  |  |  |  |  |  |  |  | **x** | **x** |  |  |
| Relatório Parcial |  |  |  |  |  |  | **x** | **x** |  |  |  |  |
| Apresentação no SIC |  |  | **x** |  |  |  |  |  |  |  |  |  |
| Relatório Final |  |  |  |  |  |  |  |  |  |  | **x** | **x** |

1. **Bibliografia**

Wong, T. G. (2022). *The Introduction to Classical and Quantum Computing*. Rooted Grove.

Johansson, N., & Larsson, J.-Å. (2019). Quantum Simulation Logic, Oracles, and the Quantum Advantage. *Entropy*, 21(8), 76.

Deustsch-Jozsa Algorithm. Qiskit, 2022. Disponível em: <https://learn.qiskit.org/course/ch-algorithms/deutsch-jozsa-algorithm>. Acesso em: 16, 08, 2023.

Grover’s Algorithm. Qiskit, 2021. Disponível em: <https://learn.qiskit.org/course/ch-algorithms/grovers-algorithm>. Acesso em: 16, 08, 2023.

Bellare, M., & Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. *Association for Computing Machinery*, *CCS '93*(1), 12.

NATION, Paul. Finding Waldo using Grover Search. IBM Quantum Enabling Technologies, 2023. Disponível em: <https://quantum-enablement.org/posts/2023/2023-07-05-Finding_Waldo_with_Grover_Search.html>. Acesso em: 16, 08, 2023.