**Centro Universitário do Instituto Mauá de Tecnologia  
Escola de Engenharia Mauá**Engenharia de Computação

Rodrigo Machado Pedreira

**Implementação e comparação de circuitos lógicos clássicos e quânticos em Python**

São Caetano do Sul  
2023

Rodrigo Machado Pedreira

**Implementação e comparação de circuitos lógicos clássicos e quânticos em Python**

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia Mauá do Centro Universitário do Instituto Mauá de Tecnologia como requisito parcial para a obtenção do título de Engenheiro de Computação.

Orientador: Dr. Prof. Sandro Martini

Área de concentração: Engenharia de Computação

São Caetano do Sul  
2023

|  |  |
| --- | --- |
|  | Pedreira, Rodrigo  Título principal : subtítulo. / Rodrigo Machado Pedreira. — São Caetano do Sul : CEUN-IMT, 2023.  Número de páginas p.  Trabalho de Conclusão de Curso – Escola de Engenharia Mauá do Centro Universitário do Instituto Mauá de Tecnologia, São Caetano do Sul, SP, 2023.  Orientador(a): Dr. Prof. Sandro Martini  1. Palavra-chave1. 2. Palavra-chave2. 3. Palavra-chave3. 4. Palavra-chave4. 5. Palavra-chave5. I. Instituto Mauá de Tecnologia. Escola de Engenharia. II. Título. |

Rodrigo Machado Pedreira

**Implementação e comparação de circuitos lógicos clássicos e quânticos em Python**

Trabalho de Conclusão de Curso aprovado pela Escola de Engenharia Mauá do Centro Universitário do Instituto Mauá de Tecnologia como requisito parcial para a obtenção do título de Engenheiro de Computação.

Banca avaliadora:

Dr. Prof. Sandro Martini  
Orientador(a)

Nome completo do professor(a) avaliador(a) 1 e título   
Avaliador(a) ou Instituição, se externo

Nome completo do professor(a) avaliador(a) 2, se houver, e título   
Avaliador(a) ou Instituição, se externo

São Caetano do Sul, data da apresentação de mês de 2023.

*Dedicamos este trabalho para   
pessoa ou pessoas às quais o trabalho é dedicado.*

Agradecimentos

*A epígrafe é texto contendo um pensamento ou uma ideia,  
 em português ou em outro idioma alusivo ao conteúdo ou experiência do trabalho,   
com a devida citação de seu autor.*

Resumo

Palavras‑chave: Palavra‑chave1. Palavra‑chave2. Palavra‑chave3. Palavra‑chave4. Palavra‑chave5.

*Abstract*

Keywords: Keyword1. Keyword2. Keyword3. Keyword4. Keyword5

Lista de figuras

**No table of figures entries found.**

Lista de tabelas

Lista de abreviaturas e siglas

~~IA – Inteligência Artificial~~

~~MIT –~~ *~~Massachusetts Institute of Technology~~*

~~P&D – Pesquisa e Desenvolvimento~~

~~Lista de símbolos~~

Sumário

[1 Introdução 27](#_Toc134737848)

[1.1 Relação com a mecanica quântica 27](#_Toc134737849)

[1.2 origem 27](#_Toc134737850)

[1.3 Corrida entre países para supremacia quântica 29](#_Toc134737851)

[1.4 Expectativas para o mundo coorporativo 29](#_Toc134737852)

[1.5 Objetivos 31](#_Toc134737853)

[1.6 ~~Justificativa~~ 31](#_Toc134737854)

[1.7 Organização do trabalho 31](#_Toc134737855)

[2 Fundamentos da computação clássica 33](#_Toc134737856)

[2.1 sistemas digitais 33](#_Toc134737857)

[2.2 Portas logicas clássicas 33](#_Toc134737858)

[2.2.1 Porta AND 33](#_Toc134737859)

[2.2.2 Porta OR 33](#_Toc134737860)

[2.2.3 Porta NOT 33](#_Toc134737861)

[2.2.4 Porta NAND, NOR, XOR e XNOR 33](#_Toc134737862)

[2.3 Circuitos combinacionais e sequenciais 33](#_Toc134737863)

[3 Fundamentos da Computação Quântica 35](#_Toc134737864)

[3.1 Mecânica quântica e qubits 35](#_Toc134737865)

[3.2 Princípios de superposição e entrelaçamento 35](#_Toc134737866)

[3.3 Portas lógicas quânticas 35](#_Toc134737867)

[3.3.1 Porta de Pauli-X 35](#_Toc134737868)

[3.3.2 Porta de Pauli-Y 35](#_Toc134737869)

[3.3.3 Porta de Pauli-Z 35](#_Toc134737870)

[3.3.4 Porta Hadamard 35](#_Toc134737871)

[3.3.5 Portas CNET, Toffoli e outras 35](#_Toc134737872)

[3.4 Circuitos quânticos e algoritmos 35](#_Toc134737873)

[4 Simulação em Python 37](#_Toc134737874)

[4.1 Introdução ao Python 37](#_Toc134737875)

[4.2 Simulação de portas lógicas clássicas 37](#_Toc134737876)

[4.2.1 Implementação das portas lógicas 37](#_Toc134737877)

[4.2.2 Exemplos de simulações e análise 37](#_Toc134737878)

[4.3 Simulação de portas lógicas quânticas 37](#_Toc134737879)

[4.3.1 Introdução a bibliotecas quânticas em Python 37](#_Toc134737880)

[4.3.2 Implementação das portas lógicas quânticas 37](#_Toc134737881)

[4.3.3 Exemplos de simulações e análise 37](#_Toc134737882)

[5 Comparação entre Computação Clássica e Quântica 39](#_Toc134737883)

[5.1 Vantagens e desvantagens 39](#_Toc134737884)

[5.2 Aplicações e implicações práticas 39](#_Toc134737885)

[5.3 Desafios e perspectivas futuras 39](#_Toc134737886)

[6 Conclusão 41](#_Toc134737887)

[6.1 Síntese dos resultados 41](#_Toc134737888)

[6.2 Contribuições do trabalho 41](#_Toc134737889)

[6.3 Sugestões para trabalhos futuros 41](#_Toc134737890)

[Referências 42](#_Toc134737891)

[Glossário 43](#_Toc134737892)

[Apêndice a – Códigos das simulações em Python 44](#_Toc134737893)

[Anexo 45](#_Toc134737894)

[Índice 46](#_Toc134737895)

# Introdução

Essa seção contém uma breve apresentação do tópico e descreve a relevância do tópico, os objetivos do trabalho e a abordagem utilizada.

## Relação com a mecanica quântica

Computadores quânticos usam fenômenos da mecânica quântica afim de operar de uma forma impossível para computadores clássicos. De acordo com a teoria quântica, matéria física em escalas muito pequenas, níveis subatômicos, se comporta de maneira única, diferente da física clássica que rege o mundo como o percebemos. A melhor maneira de descrever essa peculiaridade é dizer que estas entidades quânticas, ou partículas subatômicas, podem exibir comportamento de partículas e de ondas. Essa dualidade foi aptamente nomeada princípio da dualidade onda-partícula.

Outro conceito importante é o da superposição. A superposição se refere habilidade de uma partícula quântica de existir em múltiplos estados ao mesmo tempo, algo totalmente contraintuitivo do entendimento humano do mundo observável descrito pela física clássica, onde partículas só podem existir em um estado por vez. Devido a esse comportamento não é possível prever com certeza o estado de um sistema quântico somente calcular a probabilidade de estar em quais estados. É possível medir seu estado em um determinado instante de tempo, porém ao realizar a medição no próximo instante a partícula já estará em outro estado e torna-se impossível calcular estados anteriores à medida.

Essa propriedade da superposição e do cálculo probabilístico permite que computadores quânticos executem certos procedimentos exponencialmente mais rápido que computadores clássicos.

## Origem

Antes da noção de fundir computadores com teoria quântica existir havia um campo de estudo chamado ciência da informação quântica, no qual buscava-se compreender a análise, processamento e transmissão de informação por meio de princípios da mecânica quântica. Foi deste campo que se derivou a ideia de computação quântica.

Em 1980 o físico Paul Benioff descreveu o primeiro modelo mecânico quântico computacional e demonstrou que um computador poderia operar sobre as leis da mecânica quântica (BENIOFF, 1980).

No ano seguinte, 1981, na primeira conferência de física da computação sediada no *Massachusetts Institute of Technology* (MIT), Benioff provou que é possível um computador operar sobre as leis da física quântica ([BENIOFF\_1982]). Na mesma conferência, Richard Feynman observou que, aparentemente, é impossível simular de maneira eficiente a evolução de um sistema quântico utilizando um computador tradicional e propôs um modelo básico para um computador quântico ([FEYNMAN\_1982]).

Passado alguns anos de progresso, em 1994 o professor Peter Shor desenvolveu um algoritmo quântico, ou seja, para computadores quânticos, de fatoração de números inteiros que até hoje é relevante e considerado um dos melhores de sua categoria. Esse algoritmo teve grandes implicações para o futuro da computação quântica e será mais bem descrito na seção 1.3 a seguir.

Nos anos seguintes grandes avanços foram alcançados, entretanto devido às limitações tecnológicas ainda era muito difícil construir um computador quântico e os primeiros computadores eram mais provas de conceitos do que máquinas que pudessem ser programadas ou realizar algo útil.

Foi por volta de 2018-2020 que o progresso nesta área começou a evoluir de maneira expressiva. Houve grandes sucessos neste período, como:

1. a Google alegando que seu computador quântico conseguiu executar um algoritmo específico mais rápido que um computador clássico, algo que até então não havia sido provado na prática (GIBNEY, 2019). Todavia, deve ser mencionado que era um algoritmo especialmente criado para esta tarefa e não produzia nenhum resultado útil;
2. o lançamento um novo computador quântico e melhorias no sistema de computação cloud disponível para uso online, ambos pela IBM (SHANKLAND, 2019);
3. melhorias em simuladores de computadores quânticos e linguagem de programação (JAVADI-ABHARI *et al.*, 2019), que facilitam a criação de programas quânticos e assim permite que mais pessoas explorem esta tecnologia;
4. criação de iniciativas e investimentos por parte de governos (LANES, 2023).

Desde então a velocidade e quantidade de novas conquistas só aumenta, algumas até renderam manchetes em jornais convencionais, embora com títulos um tanto sensacionalistas.

## Corrida entre países para supremacia quântica

Tecnologias quânticas têm um enorme potencial, suficiente para revolucionar o mundo, mas ainda há um longo caminho a ser percorrido para alcançar esta meta. Por exemplo, computadores quânticos têm a capacidade de realizar algumas tarefas bem definidas que são impossíveis em computadores clássicos, ou em outros casos completá-las exponencialmente mais rápido.

Tarefas como fatorar números inteiros muito grandes, algo viável graças ao Algoritmo de Shor, desenvolvido por Peter Shor na Bell Labs (SHOR, 1994). Esse algoritmo tem o poder de quebrar sistemas criptográficos de chave pública em tempo polinomial, isso tem enormes implicações, pois estes sistemas são essenciais para segurança digital. Consequentemente, após a descoberta de Shor, esse campo ~~esotérico~~ puramente teórico, que antes era reservado à cientistas entusiastas, atraiu a atenção de instituições governamentais de potencias globais e gigantes empresas de tecnologia, como o Departamento de Defesa Americano e a IBM.

Nações mais desenvolvidas estão incentivando a pesquisa e desenvolvimento (P&D) desta inovação, devido aos riscos para segurança nacional e os benefícios ofertados por esta tecnologia. Não só oferta a capacidade de violar certos sistemas criptográficos com o algoritmo de Shor, mas é, também, possível utilizá-la para criptografar e transmitir dados.

O governo da China se comprometeu em investir US$ 15,3 bilhões em P&D nesta área, mais que o dobro dos US$ 7,2 bilhões pela União Europeia. Os Estados Unidos da América (EUA) seguem em terceiro lugar no ranking dos maiores investidores com US$ 1,9 bilhões, em contrapartida, os EUA lideram em investimentos do setor privado (LANES, 2023).

## Expectativas para o mundo coorporativo

A *Boston Consulting Group* (BCG), uma renomada empresa de consultoria empresarial e dentre as três com maior receita, já publicou diversas análises sobre computação quântica e destaca a importância de empresas acompanharem esta área. A empresa afirmou em 2018 que “Toda empresa precisa entender como descobertas na computação quântica vão afetar os negócios.” (GERBERT e RUESS, 2020), tradução do autor, e alertou em 2023 “O maior desafio pode ser [encontrar] empregados de qualidade, dadas as restrições de oferta. Empresas precisam de uma estratégia de talento compreensiva que engloba a contratação ou desenvolvimento de líderes a par da computação quântica, operadores versados e funcionários experts em computação quântica. Formar empregados competentes dentro das empresas levará tempo, então é melhor começar o quanto antes possível.” (LANGIONE *et al.*, 2023), tradução do autor.

Além disso, a *McKinsey & Company*, outra empresa de consultoria empresarial que desfruta de ainda mais prestígio que a BCG, julgou que computação quântica tem tamanho potencial que a identificou como uma das 3 maiores próximas tendencias de tecnologia. A empresa segue dizendo que computação quântica sozinha, uma dentre as três principais áreas emergentes da tecnologia quântica, pode contabilizar quase US$ 1,3 trilhões em valor até 2035 (MCKINSEY, 2023).

Neste mesmo relatório a corporação relata uma pesquisa, realizada pelos próprios, em que para cada 3 vagas de emprego no setor de tecnologia quântica há apenas um profissional qualificado para assumir o cargo. Até 2025 a firma prevê que menos de 50 % das vagas de trabalhos na área serão ocupadas, salvo uma mudança significativa da quantidade de profissionais ou na previsão de ofertas de emprego (MCKINSEY, 2023).

(Mai, 2022) Haim Israel, the managing director of research at Bank of America declared that quantum computing will be “bigger than fire” at Commercialising Quantum conference.

Funding for quantum start-ups doubled in 2021  
Our research finds that funding of start-ups focused on quantum technologies more than doubled—from $700 million in 2020 to $1.4 billion in 2021  
Chart, line chart

Description automatically generated Será removida!  
Lembrar de mencionar footnote2 da imagem.

## Objetivos

O objetivo geral deste trabalho é apresentar os princípios básicos do funcionamento da computação quântica, suas aplicações, limitações e o impacto na sociedade de sua utilização.

Para alcançar este objetivo, foram propostas 3 abordagens:

1. explorar o que é computação clássica e quântica e explicar os conceitos teóricos fundamentais;
2. comparar computação clássica com quântica e destacar vantagens, desvantagens e limitações;
3. apresentar um algoritmo quântico que demonstra em pratica a aplicação da teoria abordada por este trabalho. é escrito em linguagem de programação Python e pode ser executado tanto em um computador quântico quanto um simulador.

## ~~Justificativa~~

## Organização do trabalho

# Fundamentos da computação clássica

## Sistemas digitais

## Portas logicas clássicas

### Porta AND

### Porta OR

### Porta NOT

### Porta NAND, NOR, XOR e XNOR

## Circuitos combinacionais e sequenciais

# Fundamentos da Computação Quântica

Quotes legais no ChatGPT

## Mecânica quântica e qubits

## Princípios de superposição e entrelaçamento

## Portas lógicas quânticas

### Porta de Pauli-X

### Porta de Pauli-Y

### Porta de Pauli-Z

### Porta Hadamard

### Portas CNET, Toffoli e outras

## Circuitos quânticos e algoritmos

# Simulação em Python

## Introdução ao Python

## Simulação de portas lógicas clássicas

### Implementação das portas lógicas

### Exemplos de simulações e análise

## Simulação de portas lógicas quânticas

### Introdução a bibliotecas quânticas em Python

### Implementação das portas lógicas quânticas

### Exemplos de simulações e análise

# Comparação entre Computação Clássica e Quântica

## Vantagens e desvantagens

## Aplicações e implicações práticas

## Desafios e perspectivas futuras

# Conclusão

## Síntese dos resultados

## Contribuições do trabalho

## Sugestões para trabalhos futuros

###### Referências

[[BENIOFF\_1982]]

[[FEYNMAN\_1982]]

BENIOFF, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. **Journal of Statistical Physics**, v. 22, n. 5, p. 563–591, 1 May 1980. ISSN 1572-9613. Disponível em: https://doi.org/10.1007/BF01011339. Acesso em: 11 May 2023.

GERBERT, P.; RUESS, F. The Next Decade in Quantum Computing—and How to Play. **BCG**, 19 August 2020. Disponível em: https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play. Acesso em: 8 May 2023.

GIBNEY, E. Hello quantum world! Google publishes landmark quantum supremacy claim. **Nature**, v. 574, p. 461–462, 23 October 2019. Disponível em: https://www.nature.com/articles/d41586-019-03213-z. Acesso em: 5 May 2023.

JAVADI-ABHARI, A.; MCKAY, D.; PISTOIA, M.; WOOD, C. What’s New in Qiskit 0.9 and Why Is It Already 0.10? **Qiskit**, 14 maio 2019. Disponível em: https://medium.com/qiskit/whats-new-in-qiskit-0-9-e875f96ca695. Acesso em: 11 maio 2023.

LANES, O. Quantum Computing Is the Future, and Schools Need to Catch Up. **Scientific American**, 15 mar. 2023. Disponível em: https://www.scientificamerican.com/article/quantum-computing-is-the-future-and-schools-need-to-catch-up/. Acesso em: 5 May 2023.

LANGIONE, M.; FANCOIS BOBIER, J.; AMIT, K.; GOUREVITCH, A. Quantum Computing Is Becoming Business Ready. **BCG**, 27 April 2023. Disponível em: https://www.bcg.com/publications/2023/enterprise-grade-quantum-computing-almost-ready. Acesso em: 8 May 2023.

MCKINSEY. What is quantum computing? **McKinsey**, 01 maio 2023. Disponível em: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing. Acesso em: 8 May 2023.

SHANKLAND, S. IBM's biggest-yet 53-qubit quantum computer will come online in October. **CNET**, 18 set. 2019. Disponível em: https://www.cnet.com/tech/computing/ibm-new-53-qubit-quantum-computer-is-its-biggest-yet/. Acesso em: 11 maio 2023.

SHOR, P. W. **Algorithms for quantum computation:** discrete logarithms and factoring. *In*: Proceedings 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, USA: IEEE. November 1994. p. 124–134.

SUTOR, R. S. **Dancing with qubits:** how quantum computing works and how it may change the world. Birmingham Mumbai: Packt, 2019. ISBN 978-1-83882-736-6.

###### Glossário

* **Bit:**
* **Qubit:**

###### Apêndice a – Códigos das simulações em Python

###### Anexo

###### Índice

I