



FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA

Palavras chave: Computação Quântica, Computação, Mecânica Quântica

Autores:

SAUL VICTOR DE CASTRO E SILVA [FEEC/UNICAMP]

Prof. ROMIS ATTUX [FEEC/UNICAMP]

Introdução

No final do século XIX e início do século XX, os matemáticos Richard Dedekind e Georg Cantor deram início ao estudo da teoria dos conjuntos. Tais estudos, especialmente os de Cantor, influenciaram outro matemático muito importante do século passado: Alan Turing, que desenvolveu não apenas a teoria matemática que está por trás da computação, mas também se envolveu na construção de alguns dos primeiros computadores da história.

Paralelamente, aproximadamente na mesma época, começou o estudo de uma nova área da física: a física quântica. O trabalho de Max Planck marca o início dessa nova física, mas também devem ser destacadas as contribuições pioneiras de Albert Einstein, Niels Bohr e outros. Os estudos dessa "primeira geração" serviram de alicerce para o desenvolvimento do que veio a ser chamado de mecânica quântica, que tem o potencial de revolucionar a tecnologia como é conhecida hoje, incluindo um novo ramo da computação. De fato, a computação quântica utiliza princípios como *superposição* e *emaranhamento* para realizar seus processos de forma potencialmente mais rápida e eficiente que aquela trazida pelo paradigma digital vigente.

Alguns dos mais brilhantes físicos da história trabalharam no desenvolvimento da mecânica quântica, como Werner Heisenberg, Erwin Schrödinger, Paul Dirac e Richard Feynman. Feynman foi também um dos primeiros a levantar teorias sobre o desenvolvimento de computadores utilizando os princípios e fundamentos da mecânica quântica, argumentando que, dessa forma, os computadores seriam mais rápidos e capazes de simular diversos fenômenos naturais. Inicialmente, isso representou um grande desafio, tanto

devido à falta de tecnologia quanto à falta de conhecimento teórico necessário para o desenvolvimento desse tipo de computador.

Apesar de alguns cientistas da época acreditarem no desenvolvimento da computação quântica, foi necessário desenvolver várias teorias para correlacionar e explicar como a mecânica quântica poderia ser aplicada na teoria computacional. Com isso, no começo da década de 70, o físico Charles Bennett mostrou a existência de máquinas de Turing reversíveis, sendo a reversibilidade uma ideia central na física quântica. Na década de 80, Edward Fredkin e Tomaso Toffoli mostraram a existência de portas lógicas universais reversíveis. Esses estudos, então, mostraram a reversibilidade de modelos de computadores, mas, além disso, ainda era preciso mostrar o real potencial de um computador quântico. Com isso em mente, também na década de 80, Paul Benioff mostrou que processos computacionais quânticos conseguiam ser tão potentes quanto processos clássicos. Dessa forma, desenvolveu-se gradualmente um corpo teórico ligado à nova computação.

Embora esses estudos tenham sido realizados há mais de 40 anos, em 2023, a computação quântica ainda é uma área em processo de crescimento, e seu desenvolvimento tem ocorrido de forma notável. Por isso, há um amplo campo de estudo e desenvolvimento, tanto teórico quanto prático. O trabalho realizado nesta pesquisa é, assim, relevante por seu caráter formativo e por fornecer material para auxiliar novos estudantes nesse campo.

Metodologia

A metodologia deste trabalho foi dividida em três partes: primeiramente, foi feito um estudo sobre os princípios e fundamentos da mecânica quântica; depois foi realizado um estudo sobre computação clássica e, finalmente, foi possível adentrar os estudos introdutório sobre computação quântica.

Mecânica Quântica

Os estudos sobre mecânica quântica foram realizados utilizando o livro [Griffiths, 1995]. Esses estudos se iniciaram a partir da análise da função de onda $\Psi(x, t)$ de uma partícula, que é obtida a partir da solução da equação de Schrödinger, equação (1). O estudo dessa equação trouxe conceitos importantes: interpretação estatística da função de onda, normalização, momento e vínculos com o princípio da incerteza.

$$i\hbar \frac{\partial \Psi}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2 \Psi}{\partial x^2} + V\Psi \quad (1)$$

Logo após, foi possível estudar a equação de Schrödinger independente do tempo, mostrada na equação (2), e a solução dessa equação para vários potenciais: o **potencial do poço quadrado infinito**, o **oscilador harmônico** e a **partícula com potencial livre**.

$$-\frac{\hbar^2}{2m} \frac{d^2\psi}{dx^2} + V\psi = E\psi \quad (2)$$

Foi então possível estudar as bases do formalismo da mecânica quântica, incluindo notações, terminologias e base matemática necessárias. Aqui foi necessário revisitar elementos do estudo da álgebra linear à luz da **notação de Dirac**, ou **notação Bra-Ket**.

Computação Clássica

Para os estudos sobre computabilidade, foi utilizado como base o clássico artigo [A. M. Turing, 1936]. Primeiro, foi preciso fazer um breve estudo sobre teoria de conjuntos para entender as motivações de Turing ao teorizar sobre **computabilidade**.

Logo após, foi realizada uma discussão sobre **números computáveis**, **máquinas de Turing** e sobre como Turing chegou à idealização do que seria computabilidade num sentido amplo.

Computação Quântica

Finalmente, os livros [Gruska, 2011] e [Gyongyosi e Imre, 2019] foram utilizados para estudar as bases computação quântica. Esse estudo se iniciou com uma comparação entre a **Máquina de Turing Probabilística** e a **Máquina de Turing Quântica**. Logo após, já foi possível estudar os elementos que compõem a computação quântica.

Assim como na computação clássica, um *bit* é a unidade de informação utilizada; na computação quântica, a unidade de informação recebe o nome de *qubit*, ou seja, um bit quântico, que, diferentemente dos bits clássicos, pode ser "tanto 0 como 1 ao mesmo tempo", sendo representado da seguinte forma: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Dessa forma, é possível avançar e estudar os registradores quânticos, que, similarmente aos registradores tradicionais, são os componentes que irão armazenar os qubits e prover meios para a realização de diversas operações.

É importante comentar, também, sobre o princípio do emaranhamento quântico, pois esse é um dos conceitos mais importantes na computação quântica. De uma maneira simples, para duas partículas emaranhadas, o estado quântico da 1ª partícula se vincula organicamente ao estado quântico da 2ª, independentemente da distância entre elas. Assim, ao determinar o estado de uma partícula, adquire-se total conhecimento sobre o estado quântico da outra. Para a computação quântica isso é muito importante, pois permitiria a troca de informação de uma forma instantânea.

Foi possível também introduzir os circuitos quânticos, que representam a forma de se conectar portas lógicas quânticas para construir um computador quântico.

Tendo sido finalizados esses estudos, foram realizadas outras pesquisas com o intuito de construir

uma taxonomia de abordagens para construção de hardware em computação quântica; além das áreas onde essa nova tecnologia pode ser aplicada como: **criptografia, otimização, inteligência artificial, simulações quânticas** etc.

Conclusões e Perspectivas Futuras

A partir do que foi estudado, foi possível montar um arcabouço de princípios e fundamentos da computação quântica. O esforço para estudar mais a fundo a noção de computabilidade foi de extrema importância, pois possibilitou um entendimento melhor sobre as limitações que a computação clássica têm e por que a computação quântica pode superar algumas dessas limitações.

As pesquisas finais realizadas mostraram os diferentes ramos de aplicação da computação quântica, que são alguns dos ramos que estão sendo estudados para ajudar no avanço dessa área. Esses estudos foram feitos como uma motivação, para que novos estudos sejam feitos e que se dê continuidade a esse ramo de pesquisa. No relatório final, detalharemos mais esses estudos em andamento.

Bibliografia

[Gruska, 2011] J. Gruska, Quantum Computing, McGraw-Hill, 2011.

[Griffiths, 1995] D. J. Griffiths, Introduction to Quantum Mechanics, Prentice Hall, 1995.

[Gyongyosi e Imre, 2019] L. Gyongyosi, S. Imre, "A Survey on Quantum Computing Technology", Computer Science Review, Vol. 31, pp. 51 - 71, 2019.

[A. M. Turing, 1936] A. M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem", Proceedings of the London Mathematical Society, Series 2, pp. 230-265, 1936.