MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
(Real Academia de Artilharia, Fortificação e Desenho/1792)
CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

Victor Villas Bôas Chaves

Algoritmos em Computação Quântica

Rio de Janeiro
2015

Resumo

O presente trabalho apresenta um estudo sobre sistemas determinísticos, sistemas probabilísticos, sistemas quânticos, qubits e portas lógicas quânticas. Paralelamente ao estudo, foi implementado na linguagem de programação python programas para cálculos e simulações de sistemas quânticos.

Palavras Chave: Algoritmos, Computação Quântica

1 Introdução

1.1 Justificativa

Na computação clássica o computador é baseado na arquitetura de Von Neumann que faz uma distinção clara entre elementos de processamento e armazenamento de dados, isto é, possui processador e memória destacados por um barramento de comunicação, sendo seu processamento sequencial.

Entretanto os computadores atuais possuem limitações, como por exemplo, na área de Criptografia e Segurança de Dados, onde não existem computadores com potência ou velocidade de processamento suficiente para suportar algoritmos de alta complexidade. Dessa forma surgiu a necessidade da criação de um computador diferente dos usuais que resolvesse problemas como a fatoração de números primos muito grandes, logaritmos discretos e simulação de problemas da Física Quântica.

E assim os estudos em Computação Quântica se tornaram muito importantes e a necessidade do desenvolvimento de uma máquina extremamente eficiente se torna maior a cada dia.

Na computação quântica a unidade de informação básica é o Bit quântico ou q-bit. O fato de a computação quântica ser tão poderosa está no fato de que além de assumir '0' ou '1' como na computação clássica, ela pode assumir ambos os estados '0' e '1' ao mesmo tempo.

E é graças a essa propriedade da superposição de estados que motivou os estudos em computação quântica. Se na computação clássica o processamento é sequencial, na computação quântica o processamento é simultâneo.

A computação quântica é um assunto que está começando a ser estudado na esfera global, embora o computador quântico seja incipiente, já existem alguns algoritmos quânticos, como por exemplo, o algoritmo de Shor para fatoração e algoritmo de Grover para acelerar o processo de procura em banco de dados.

Os algoritmos quânticos abrem portas para complexidades inferiores aos já existentes, o que futuramente terá impacto direto em criptografia, assinatura digital, sistemas de cartões de crédito e segurança digital de modo geral, pois com tais algoritmos será possível tratar os problemas np-completos (para os quais não se conhece solução polinomial) por uma nova esfera.

1.2 Objetivos

Este projeto tem como objetivo a análise de caráter geral e o desenvolvimento de algoritmos computacionais quânticos, bem como a comparação com algoritmos da computação tradicional, para resolução de problemas da literatura convencional.

2 Desenvolvimento

2.1 Cronograma

O desenvolvimento da pesquisa tem o seguinte planejamento:

1. Pesquisa bibliográfica do princípio de funcionamento de um computador quântico.
2. Pesquisa sobre as diferenças na programação de algoritmos quânticos em relação à programação binária tradicional.
3. Análise dos algoritmos quânticos específicos.
4. Estudo comparativo dos algoritmos quânticos com os respectivos algoritmos do paradigma tradicional.

Com base nessas atividades, o seguinte cronograma é previsto para o projeto:

Atividade	1º Trimestre	2º Trimestre	3º Trimestre	4º Trimestre
1	X			
2	X	X		
3		X	X	
4			X	X

Tabela 1 – Distribuição de atividades

2.2 Atividades

O livro utilizado para construir a base teórica necessária foi o Quantum Computing for Computer Scientists (YANOFSKY; MANNUCCI, 2008), do qual os capítulos 1, 2, 3, 4 e 5 foram estudados. Três apresentações foram feitas para o orientador, das quais a primeira abrangeu os capítulos 1 e 2, a segunda abrangeu o capítulo 3 e a terceira o capítulo 4.

3 Resultados

Referências

YANOFSKY, N. S.; MANNUCCI, M. A. *Quantum Computing for Computer Scientists*. 1. ed. New York: Cambridge University Press, 2008.