SIMULAÇÃO DA TRANSFORMADA QUÂNTICA DE FOURIER COM O SIMULADOR ZENO

José Filipe de Lima, Rodrigo Soares Semente

Departamento de Ciências Exatas e Naturais (DCEN) - Universidade Federal Rural do Semi-Árido (UFERSA)

filipe_lima2013@outlook.com, rodrigo.semente@ufersa.edu.br

Abstract: *Quantum computing has been extensively studied over the last few years. It has just been proving to be a very promising technology for the development of computing. This work aims to talk about concepts involved for a quantum computation performance. For that, a review of the existing literature on the subject was carried out, in order to obtain the knowledge developed about it until the moment. There is talk about q-bits, which is a fundamental unit of quantum computing information, and its assets. Some of the quantum logical versions are presented that are fundamental for a computational performance. A brief introduction on a Quantum Fourier Transform (TQF) and its computational form for a vector. It is the Zeno quantum circuit simulator and a DFT algorithm simulation, as well as the possibility of implementing other algorithms in it.*

Keywords: *Quantum Computation, TQF, Zeno Quantum Simulator.*

Resumo: *A computação quântica vem sendo amplamente estudada ao longo dos últimos anos. A mesma vem mostrando-se uma tecnologia bastante promissora para o desenvolvimento da computação. Este trabalho tem como objetivo falar sobre os conceitos envolvidos para a realização da computação quântica. Para tal, foi realizada uma revisão da literatura existente sobre o tema afim de se obter o conhecimento desenvolvido sobre o mesmo até o momento. Fala-se sobre os q-bits, que é a unidade fundamental de informação da computação quântica, e suas propriedades. Em seguida são apresentadas algumas das portas lógicas quânticas que são fundamentais para a realização da computação. É apresentada uma breve introdução sobre a Transformada Quântica de Fourier (TQF) e sua forma de cálculo para um vetor ket. É apresentado o simulador de circuitos quânticos Zeno e a simulação do algoritmo da DFT, bem como possibilidade implementação de outros algoritmos no mesmo.*

Palavras chave: *Computação Quântica, TQF, Simulador Quântico Zeno.*

1. Introdução

Com a evolução da tecnologia, vendo crescendo a necessidade de computadores que possuam uma capacidade de processamento cada vez maior. Entretanto, os aspectos físicos que possibilitam a computação clássica impõem um limite para a capacidade que os computadores clássicos podem alcançar. Isso se deve ao fato de que o número de elétrons que podem ser colocados em uma determinada área tem um valor limite GULGELMIN (2013). Assim surge a necessidade de uma nova tecnologia que gere uma revolução na computação, assim como o computador clássico gerou em seu desenvolvimento. Uma tecnologia que vem se mostrando muito promissora e que pode ser capaz de gerar essa revolução é a computação quântica. Seu princípio de funcionamento baseia-se na codificação de informação em sistemas quânticos. Estados de sistemas quânticos são usados para representar bits de informação que recebem o nome de q-bits. Os computadores quânticos utilizam as propriedades dos sistemas quânticos, tais como a superposição de estados, para aumentar a velocidade de processamento. Os estudos da computação quântica se intensificaram quando os primeiros algoritmos específicos para computadores quânticos foram desenvolvidos. Esses algoritmos são o algoritmo de Shor e o de Grover. Neste trabalho é feita a simulação do algoritmo da Transformada Quântica de Fourier (TQF) para vetores ket. Esse circuito quântico é usado no algoritmo de fatoração de Shor PORTUGAL et al (2004). É feita a simulação no simulador de circuitos quânticos Zeno e comparado os resultados das simulações com os obtidos baseados na expressão para a TQF.

A seguir são apresentados alguns conceitos básicos de Computação Quântica (CQ) que serão necessários para o entendimento da implementação dos algoritmos bem como a sua simulação.

1.1. Os q-bits quânticos

Na computação quântica, assim como na computação clássica, usa-se estados para realização do processamento de dados. Portugal (2004) aponta que em computação quântica esses estados são estados quânticos. O *bit* clássico é então substituído pelo *q-bit*. Santos (2016) aponta que, em geral, os *q-bits* são representados, de forma física, por estados ortogonais associados a qualquer sistema quântico que possua dois níveis de energia. Esses estados podem ser polarização vertical e horizontal de fótons bem como o estado de spin do elétron. Por sua vez, esses estados podem ser representados de uma forma abstrata por $|0\rangle$ e $|1\rangle$ que são os estados da base computacional. Esses estados abstratos são vetores representados por

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ e } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Essa notação para um estado quântico, representado como um vetor, é devida à Dirac. Esses vetores formam a base computacional, pois os vetores $|0\rangle$ e $|1\rangle$ formam uma base

ortonormal do espaço vetorial $\mathbb{C}^2$. Devido às propriedades da mecânica quântica podemos escrever um estado genérico $|\psi\rangle$ como uma combinação linear dos estados $|0\rangle$ e $|1\rangle$, isto é,

$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \quad (1)$$

onde α e β pertencem ao conjunto dos complexos. Isso de fato oferece uma certa vantagem em relação ao bits clássicos. Nussenzveig (2013) nos diz que a condição de normalização exige que $|\alpha|^2 + |\beta|^2 = 1$. Uma análise mais cuidadosa de (1) nos permite perceber que o estado $|0\rangle$ é uma superposição dos estados $|0\rangle$ e $|1\rangle$. Assim "precisamos de apenas uma única partícula para 'escrever' esse estado, o que não é possível em computadores clássicos" (SANTOS, 2016). Essa vantagem do computador quântico trona-se mais notável quando consideramos mais do que um único q-bit. Considerando como exemplo o estado particular de um sistema composto por dois níveis mostrado abaixo:

$$|\psi\rangle = ½(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad (2)$$

que são todas as combinações possíveis de dois bits. É importante notar que com apenas dois q-bits é possível armazenar uma quantidade que informação que, para um computador clássico, requer oito bits. Assim é perceptível que um computador quântico requer um espaço físico menor do que o computador clássico.

Mas qual o significado físico de (1)? Portugal et al. (2004) diz que fisicamente o q-bit está em ambos os estados $|0\rangle$ e $|1\rangle$ ao mesmo tempo. Dada essa propriedade, a quantidade de informação que pode ser armazenada em $|\psi\rangle$ torna-se infinita. A informação contida nesse q-bit está no nível quântico. Logo, para torna-la acessível, é necessário realizar uma medida. Mas o ato de medir um sistema quântico interfere em seu estado fazendo com que o mesmo assuma o estado $|0\rangle$, com probabilidade $|\alpha|^2$, ou o estado $|1\rangle$ com probabilidade $|\beta|^2$. Como esperado, a soma dessas probabilidades é sempre igual a 1 como já exposto pela condição de normalização. Lembrando um pouco sobre comprimento de vetores vemos que, de forma matemática, o q-bit é um vetor de módulo unitário do espaço vetorial $\mathbb{C}^2$.

1.2. Circuitos Quânticos

Assim como na computação clássica, na computação quântica também são implementados circuitos para a formação das portas lógicas. Essas portas quânticas permitem o processo de computação agrupando-as em sequência onde é aplicada uma configuração de entrada e uma configuração de saída é devolvida como resultado da computação (SANTOS, 2016). Essa entrada pode ser o produto tensorial entre os q-bits ou um estado emaranhado. A realização de algumas ações em estados quânticos faz com eles ajam como as portas lógicas dos computadores clássicos. Assim é possível estabelecer, assim como na computação clássica, portas quânticas universais. Entretanto existem algumas diferenças entre as portas clássicas e as portas quânticas. Segundo Bulnes (2005) a principal delas é que algumas operações irreversíveis na computação

clássica, como, por exemplo, AND e OR, são reversíveis na computação quântica. Na verdade, como o próprio autor destaca, todas as operações o são, uma vez que se tratam de transformações unitárias.

1.3. A Transformada de Fourier Quântica Discreta

Segundo Portugal et al (2004) Transformada de Fourier (TF) de uma função F: {0,....., N – 1} → ℂ é uma nova função F': {0,....., N – 1} → ℂ que é dada por:

$$F'(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} F(j) \quad (2.3.1)$$

Podemos aplicar a TF em uma função ou em um estado da base computacional. A TF aplicada ao estado $|k\rangle$ da base computacional $\{|0\rangle,..., |N-1\rangle\}$ é dada por:

$$DFT(|k\rangle) = |\psi_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |j\rangle, \quad (2.3.2)$$

donde o conjunto $\{ |\psi_k\rangle: k = 0,.....,N-1\}$ é uma nova base ortonormal e $N = 2^n$ onde n = número de q-bits no registrador. Vamos tomar como exemplo a DFT do ket $|0\rangle$ para um registrador com 3 q-bits dada por 2.3.2:

$$DFT(|0\rangle) = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010 + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{8}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle) \quad (2.3.3)$$

Para o Ket $|1\rangle$ temos a seguinte DFT:

$$DFT(|1\rangle) = \frac{1}{\sqrt{8}}[|000\rangle + (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}) |001\rangle + i|010 + (-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}) |011\rangle - |100\rangle - (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2}) |101\rangle - i|110\rangle + (\frac{\sqrt{2}}{2} - \frac{\sqrt{2}i}{2})|111\rangle] \quad (2.3.4)$$

Ambos os Kets serão simulado no simulador Zeno e os resultados serão comparados com estes últimos.

1.4. Simulador Zeno

O uso de simuladores é algo importantíssimo para algumas áreas do conhecimento. Para o ensino o uso de um simulador torna-se uma ferramenta poderosa para facilitar a compreensão e aprendizagem do conteúdo. Para o estudo da CQ a simulação desempenha um papel ainda mais importante uma vez que as máquinas quânticas existentes são de difícil acesso e bastante simples (SANTOS, 2017). Um simulador de circuitos quânticos permite que o usuário descreva um algoritmo quântico em termos de portas e circuitos e simule o resultado para um determinado estado. O uso de simuladores para auxiliar o estudo e desenvolvimento da CQ ajuda a superar os obstáculos inerentes ao acesso as máquinas quânticas. Neste contexto, o uso de simuladores quânticos em computadores clássicos, embora apresente limites, torna-se uma saída temporária bastante interessante (CABRAL, 2004).

Entre os simuladores usados para a simulação de circuitos quânticos está o simulador Zeno. Esse simulador foi desenvolvido como dissertação de mestrado de Gustavo Cabral na UFCG em 2004 (BARBOSA, 2007). Ele é um simulador universal que permite a criação e edição de projetos de algoritmos. Em 2007, na sua dissertação de mestrado na UFCG, Alexandre Barbosa apresentou uma extensão para o simulador Zeno tornando-o a única ferramenta do gênero capaz de fornecer uma descrição completa da linguagem de circuitos quânticos.

2. Metodologia

Para alcançar o resultado desejado foi seguida a seguinte metodologia:

1. Foi feito um levantamento bibliográfico sobre a notação de Dirac para a Mecânica Quântica e sua aplicação à Computação Quântica.
2. Foi feita também uma revisão da literatura a respeito da Computação Quântica e seus conceitos fundamentais. Buscou-se na literatura um circuito quântico capaz de calcular a DFT que fosse possível de ser implementado no simulador Zeno e fornece-se o resultado correto.
3. Foi implementado o algoritmo no simulador e comparado o resultado com o valor teórico.

3. Simulação da TF

O circuito quântico utilizado para o cálculo da DFT para o Ket $|0\rangle$ é mostrado na Figura 1.

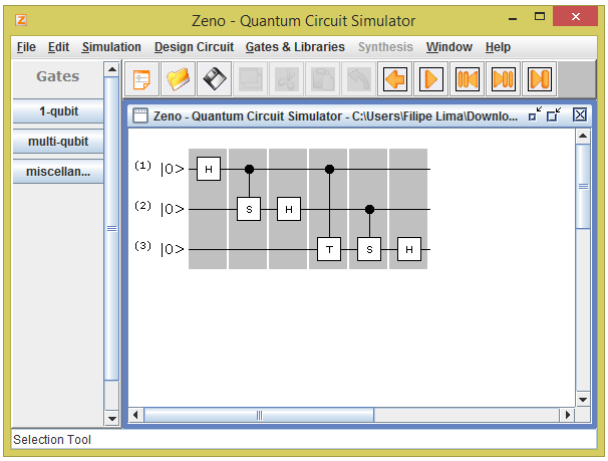

Figura 1: Circuito para simular a DFT no simulador Zeno

Neste circuito são usadas portas Hadamard (H), portas S e uma Porta T. Para um maior detalhamento dessas portas o leitor deve consultar a referência [5]. É importante também notar que são colocados alguns controles nas portas. Quando fazemos a simulação do circuito quântico obtemos o resultado que é mostrado na Figura 2.

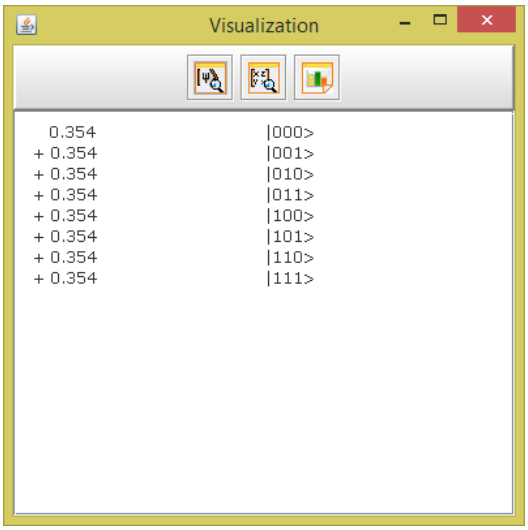

Figura 2: Resultado da simulação do circuito da DFT.

Vemos que o simulador nos dar o resultado que é previsto pela equação (2.3.3). A única diferença é que os números estão escritos em binário. O simulador Zeno consegue executar esse circuito de forma bastante rápida e eficiente. Entretanto quando tentamos simular a DFT para o Ket $|1\rangle$ obtemos o resultado mostrado na figura 3.

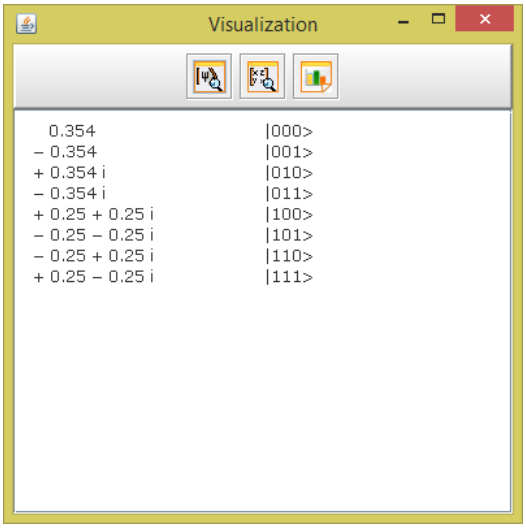

Figura 3: Simulação para o Ket $|1\rangle$

O Resultado da simulação apresenta algumas divergências para o resultado que é dado por (2.3.4). Assim, para uma implementação do algoritmo de Shor no simulador Zeno seria necessária uma modificação no circuito. Um dos possíveis problemas pode ser uma diferença entre o circuito que foi simulado e aquele apresentado por Nielsen e Chuang (2000). Pode haver algum tipo de incompatibilidade.

Um trabalho futuro seria a correção do circuito da DFT para que o mesmo pode-se ser implementado no simulador Zeno. Isso possibilitaria um trabalho voltado para a implementação do algoritmo de Shor neste mesmo simulador.

4. Conclusão

A computação quântica vem se mostrando uma tecnologia bastante promissora. Estudar e desenvolver alguns algoritmos simples e elementares é algo importantíssimo para o desenvolvimento dos pilares da computação quântica. Mesmo circuitos simples como o da DFT podem ter uma grande utilidade. Além disso, a CQ é bastante atual e representa um campo de pesquisa bastante aberto. Assim estimular o seu estudo por um número cada vez maior de pesquisadores é algo essencial para estimular o desenvolvimento dessa área de pesquisa.

Desenvolver circuitos quânticos que utilizem as vantagens oferecidas pela CQ é algo bastante complicado. Não foi encontrado na literatura um método sistêmico para o desenvolvimento desses algoritmos. Um trabalho futuro interessante seria a elaboração de uma método, mais sistemático possível, que auxilia-se o pesquisador na elaboração de algoritmos. Esse método teria como principal característica desenvolvimento de algumas funções para sistemas quânticos, como, por exemplo, elevar a probabilidade de que um dado estado seja obtido ao realizar-se uma medida.

Referências

BARBOSA, Alexandre de Andrade. **Um simulador Simbólico de Circuitos Quânticos**. 2007. 90 f. Dissertação (Mestrado). Curso de Ciência da Computação, Universidade Federal de Campina Grande, Campina Grande, 2007.

BULNES, Juan J. Díaz. **Emaranhamento e separabilidade de estados em computação quântica por ressonância magnética nuclear.** 2005. 163 f. Tese (Doutorado) - Curso de Física, Centro Brasileiro de Pesquisas Físicas, Rio de Janeiro, 2005

CABRAL, Gustavo Eulalio M. **Uma ferramenta para Projeto de Simulação de Circuitos Quânticos**. 77 f. Dissertação (Mestrado). Curso de Informática, Universidade Federal de Campina Grande, Campina Grande, 2004.

M. A. Nielsen, I. L. Chuang. **Quantum Computation and Quantum information**. Cambridge University Press, 2000.

NUSSENZVEIG, H. Moysés. **Curso de Física Básica. v 4.** São Paulo: Edgard Blücher, 1998.

PORTUGAL, Renato et al. **Uma Introdução à Computação Quântica**. Notas de aula em matemática aplicada. Sociedade Brasileira de Matemática Aplicada e Computacional, São Carlos, 2004.

SANTOS, Alan C.. O Computador Quântico da IBM e o IBM Quantum Experience. **Revista Brasileira de Ensino de Física,** [s.l.], v. 39, n. 1, p.1-11, 1 set. 2016. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1806-9126-rbef-2016-0155.