Computação quântica: uma abordagem simulacional

José Vinícius do Nascimento Silva [1], Carlos Alex Souza da Silva [2]

[1] vinnyifpb@gmail.com ; [2] calex@fisica.ufc.br. IFPB – Campus Campina Grande, Av. Tranquilino Coelho Lemos, 671 – Campina Grande – PB.

RESUMO

Esse artigo apresenta um Simulador de Computação Quântica desenvolvido em linguagem de programação Java. Tal simulador foi desenvolvido através do programa PIBICT durante o ano de 2012. O aplicativo possibilita o estudo de portas e circuitos lógicos quânticos podendo servir tanto para a pesquisa em computação quântica, como para o ensino junto a iniciantes no tema.

Palavras-chave: Simulador, Computação Quântica, circuitos lógicos, qubits.

ABSTRACT

This article presents a Quantum Computing Simulator developed in Java programming language. This applicative has been developed through the PIBICT program, during the year of 2012. The study of quantum gates and circuts is possible with this simulator, in a way that this program can be used to research as well as to introducing the quantum computation theme to naive students.

Keywords: *Simulator, Quantum Computer, logic circuits, qubits.*

1 Introdução

A miniaturização dos circuitos de computadores tem sido um dos grandes objetivos das pesquisas em tecnologia desde a descoberta dos transistores. A Lei de Moore estabelece que a densidade dos transistores no interior dos circuitos integrados dobra a cada 18 ou 24 meses, dependendo da "versão da lei" que se escolhe usar (DISCO, 1998).

Entretanto, a natureza impõe um limite para este processo. Como foi colocado, pela primeira vez por Benioff (1980), abaixo de certas dimensões, os efeitos advindos da Mecânica Quântica se tornarão tão marcantes que o funcionamento do transistor poderá ser inviabilizado. Dessa forma, o limite final para a miniaturização seria a produção de um sistema que fosse regido pelas leis da Mecânica Quântica.

Richard Feynman elaborou a primeira proposta de utilizar um fenômeno quântico para executar rotinas computacionais, introduzindo o conceito de computador quântico. Segundo Feynman (1982), um computador quântico seria uma espécie de simulador hábil para fazer simulações diretas das propriedades de qualquer sistema quântico, tais como evoluções temporais unitárias, emaranhamentos e probabilidades.

O grande poder computacional que os sistemas quânticos oferecem, sendo os mesmos capazes de fazer cálculos que seriam impossíveis para um computador convencional, tem estimulado um grande número de desenvolvimentos teóricos nesta área. Entretanto, em contraste a tudo isso, a realização experimental da mesma ainda encontra muitos desafios. Muito embora algumas implementações básicas de computadores quânticos já tenham ocorrido, através de íons armadilhados (CIRAC, 1995) ou de ressonância nuclear magnética (JONES e MOSCA, 1998), e alguns algoritmos já terem sido demonstrados com sucesso (JONES, MOSCA e HANSEN, 1998), algumas dificuldades têm adiado a realização de um computador quântico útil para o futuro.

Por outro lado, a computação quântica não é o único ramo do conhecimento que possui este tipo de problema: o da inexistência de um sistema real onde se possam fazer experimentos. Isto motivou o surgimento e o contínuo desenvolvimento de uma nova ferramenta que é a modelagem computacional. Tal ramo do conhecimento trata da simulação de soluções para problemas científicos.

As simulações podem ser vistas como representações ou modelagens de objetos específicos reais ou imaginados, de sistemas ou fenômenos. Elas podem ser bastante úteis, particularmente quando a experiência original for impossível de ser reproduzida. Exemplos de tais situações podem ser uma descida na Lua, uma situação de emergência em uma usina nuclear ou mesmo um evento histórico ou astronômico (RUSSEL, 2001). Experimentos perigosos ou de realizações muito caras assim como os que envolvam fenômenos muito lentos ou extremamente rápidos estão, também, dentro da classe de eventos a serem alvos prioritários de simulações computacionais em Física.

Especificamente, em computação quântica, programas simuladores de operações têm surgido como ferramentas bastante úteis no estudo e no desenvolvimento de tal ciência (BARBOSA, 2008). Como exemplo, um simulador de circuitos quânticos permite descrever (textualmente e/ou graficamente) um algoritmo quântico em termos de portas e circuitos e testar esse algoritmo para um estado quântico específico, através da simulação do hardware assim descrito.

Diante de tudo isso há uma grande necessidade em relação à produção de softwares que simulem fenômenos de computação quântica, no sentido de obtermos um melhor entendimento da mesma. Objetivamos, então, através desse artigo, apresentar a produção de um software de simulação de operações quânticas, desenvolvido no sentido de obter uma ferramenta útil para o ensino e para a pesquisa nessa área do conhecimento.

Este artigo está organizado como se segue: na seção 2, faremos uma breve revisão de computação clássica; na seção 3, explicaremos os conceitos relacionados à computação quântica; na seção 4, apresentaremos o simulador de circuitos quânticos desenvolvido em nosso trabalho; a seção 5 é destinada a conclusões e perspectivas.

2 Computação clássica

O computador tal qual o conhecemos atualmente é baseado na arquitetura de Von Neumann. Um computador de Von Neumann faz uma distinção clara entre elementos de processamento e armazenamento de informações, isto é, possui processador e memória separados por um barramento de comunicação. Mais especificamente, destacam-se duas características em particular sobre um computador

de Von Neumann: a organização da memória e o método de processamento.

As palavras de memória podem conter tanto instruções como dados. O processamento, por sua vez, é sequencial, podendo conter desvios condicionais ou incondicionais. O reflexo dessas características nos computadores que temos na prática é a existência do "program counter" (que é incrementado a cada instrução) e da memória principal (que contém os programas executáveis e seus arquivos de dados).

Essas são as duas características mais importantes da arquitetura de Von Neumann; elas definem não apenas o computador em si, mas tudo o que está associado com ele, ou seja, desde os algoritmos que são elaborados até a eficiência com que conseguimos resolver determinados problemas.

Para ilustrar melhor a importância dessas características da arquitetura de Von Neumann, considere o exemplo a seguir. Quando um programador implementa um software, computacionalmente, ele está escrevendo um algoritmo para solucionar determinado problema. A forma como a maioria dos programadores pensa e imagina essa solução é de forma sequencial, não apenas porque pensamos dessa forma, mas porque os computadores que construímos e utilizamos há cinquenta anos também trabalham assim. A programação (estruturada, lógica ou funcional) e o processamento sequencial são consequências diretas da arquitetura de Von Neumann.

Mesmo novos paradigmas de programação, como a Orientação a Objetos, ainda estão restritos ao sistema de Von Neumann. Essa forma de organizar o computador, apesar de impor algumas restrições, é extremamente eficiente para a maioria das aplicações de um computador moderno.

Provavelmente não existe forma melhor de realizar cálculos matemáticos, editar textos, armazenar bancos de dados ou acessar a Internet; um computador de Von Neumann é a melhor máquina para executar essas tarefas. Entretanto, para algumas áreas específicas, como a Inteligência Artificial, por exemplo, talvez seja necessário um novo instrumento computacional. De fato, os programas de Inteligência Artificial mais avançados do mundo estão muito longe de alcançar algo semelhante à inteligência humana. O que faz com que nós nos perguntemos se a lógica computacional clássica é suficiente para cumprirmos tal tarefa.

Dessa forma, a culpa por não se conseguir uma inteligência artificial de alto nível não pode ser atribuída somente ao hardware. O problema da IA pode ser tanto de software como de hardware. Não se pode afirmar somente que não existem programas ou máquinas inteligentes porque os computadores atuais não têm potência ou velocidade de processamento suficiente para suportar uma Inteligência Artificial avançada. O problema pode estar relacionado à nossa falta de conhecimento para elaborar os algoritmos necessários. Assim, pode estar acontecendo de os processadores atuais serem até mais que suficientes para executar uma inteligência artificial ao nível da inteligência humana, mas ainda não conseguimos implementar os algoritmos. Por outro lado, a ausência desses algoritmos pode ser uma consequência da falta de computadores suficientemente poderosos. O fato é que não sabemos onde está o problema: no hardware, no software ou em ambos.

Um computador clássico pode ser descrito de forma bastante genérica como uma máquina que lê certo conjunto de dados, codificado em zeros e uns, executa cálculos e gera uma saída também codificada em zeros e uns. Esses dois dígitos formam a base binária, que permite expressar qualquer número inteiro. Os bits são processados por dispositivos eletrônicos que permitem a realização de operações básicas, em termos dos quais qualquer computação pode ser realizada.

Na próxima seção abordaremos um novo paradigma para a computação, o paradigma da lógica quântica. Como veremos, um computador quântico trará muitas vantagens em relação ao computador clássico, sendo que todos os cálculos realizados em um computador clássico também podem ser efetuados em computadores quânticos. Entretanto, o atrativo da computação quântica é a possibilidade de se ter algoritmos quânticos mais rápidos que os clássicos, para uma mesma classe de problemas.

3 Computação quântica

Richard Feynman elaborou a primeira proposta de utilizar um fenômeno quântico para executar rotinas computacionais, introduzindo o conceito de computador quântico. Segundo Feynman (1982), um computador quântico seria uma espécie de simulador hábil para fazer simulações diretas das propriedades de qualquer sistema quântico, tais como evoluções temporais unitárias, emaranhamentos ou probabilidades. Numa palestra apresentada na Primeira Conferência de Computação Física no MIT, Feynman

mostrou que um computador tradicional levaria um tempo extremamente longo para simular um simples experimento de física quântica. Por outro lado, sistemas quânticos simples podem executar enormes quantidades de cálculos num curto espaço de tempo (FEYNMAN, 1982).

De 1982, quando Richard Feynman observou que nenhum computador clássico poderia simular sistemas quânticos sem incorrer em uma degradação exponencial em seu desempenho, até 1994, quando Peter Shor publicou seu artigo "Algorithms for quantum computation: discrete logarithms and factoring", a computação quântica não passava de uma curiosidade acadêmica. O artigo de Shor (1994), no entanto, mudou radicalmente o quadro, pois apresentava um algoritmo quântico polinomial para fatorar números inteiros muito grandes, problema para o qual não se conhece algoritmo clássico eficiente (o melhor algoritmo é o superpolinomial).

Esse algoritmo e a enorme importância adquirida pelos sistemas de criptografia de chave pública (baseados na dificuldade computacional do problema da fatoração) estimularam o estudo da computação quântica, tanto na direção da construção de máquinas quânticas (computadores quânticos) quanto na direção do desenvolvimento de algoritmos quânticos.

As perspectivas de ganho parecem induzir e justificar os investimentos em ambas as direções. Um computador quântico é um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como superposição e interferência. O principal ganho desses computadores é a possibilidade de resolver, em tempo eficiente, alguns problemas que na computação clássica levariam tempo impraticável (exponencial no tamanho da entrada) como, por exemplo, a fatoração em primos de números naturais. A redução do tempo de resolução deste problema possibilitaria a quebra da maioria dos sistemas de criptografia usados atualmente. Contudo, o computador quântico ofereceria um novo esquema de canal mais seguro.

Para entender melhor o funcionamento de um computador quântico, temos que, em Mecânica Quântica, é possível que uma partícula esteja em dois ou mais estados ao mesmo tempo. Uma famosa metáfora denominada o gato de Schrodinger expressa esta realidade: imagine que um gato está dentro de uma caixa, com 50% de chances de estar vivo e 50% de chances de estar morto. Para a mecânica quântica, até abrirmos a caixa e verificarmos como está o gato, ele deve ser considerado vivo e morto, ao mesmo tempo. A esta capacidade de estar simultaneamente em vários estados chama-se superposição.

Um computador clássico tem uma memória feita de bits. Cada bit guarda um (1) ou um (0) de informação. Um computador quântico mantém um conjunto de qubits, o qual é uma generalização do bit clássico. Assim, a diferença básica entre um qubit e um bit é que um qubit pode conter um (1), um (0) ou uma superposição destes. Em outras palavras, pode conter tanto um (1) como um (0) ao mesmo tempo. O computador quântico funciona pela manipulação destes qubits.

Um computador quântico pode ser implementado com sistemas que obedeçam à natureza descrita pela mecânica quântica. Podem-se construir computadores quânticos com átomos que podem estar excitados e não excitados ao mesmo tempo, ou com fótons que podem estar em dois lugares ao mesmo tempo, ou com prótons e nêutrons, ou ainda com elétrons e pósitrons que podem ter um spin ao mesmo tempo "para cima" e "para baixo" e se movimentam em velocidades próximas a da luz. Com a utilização destes, ao invés de nano-cristais de silício, o computador quântico é menor que um computador tradicional. Uma molécula microscópica pode conter muitos milhares de prótons e nêutrons, e pode ser usada como computador quântico com muitos milhares de qubits.

Todo esse potencial que a computação quântica possui impulsionou um grande desenvolvimento teórico na área nas ultimas décadas. Este mesmo desenvolvimento passa por Feynman (1982), que em 1982 elaborou a primeira proposta de utilizar um fenômeno quântico para executar rotinas computacionais; Deutsch (1985), que em 1985, descreveu o primeiro computador quântico universal; Peter Shor (RUSSEL, 2001), que em 1994, no Bell Labs em Nova Jersey, descobriu um excelente algoritmo, que permite a um computador quântico fatorar grandes inteiros rapidamente; Grover (1996), que em 1996, no Bell Labs, descobriu o algoritmo de pesquisa em bases de dados quânticas. Em 1996 é, também, proposto o primeiro esquema para correção de erro quântico. Abaixo é mostrada uma tabela com o comparativo entre o tempo de fatoração de inteiros grandes utilizando a abordagem clássica e o algorítimo de Shor (OLIVEIRA, 2002).

Tabela 1 – Comparativo entre o tempo de execução da fatoração de inteiros grandes utilizando a abordagem clássica e o algorítimo de Shor

Comprimento do número a ser fatorado (em bits)	Tempo de fatoração por algoritmo clássico	Tempo de fatoração com o algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quatrilhões de anos	4,8 horas

Em contraste com os rápidos desenvolvimentos teóricos em computação quântica, a realização experimental da mesma ainda encontra muitos desafios. Muito embora algumas implementações básicas de computadores quânticos já tenham ocorrido, através de íons armadilhados (CIRAC, 1995) ou de ressonância nuclear magnética (JONES e MOSCA, 1998), e alguns algoritmos já terem sido demonstrado com sucesso (JONES, MOSCA e HANSEN, 1998), algumas dificuldades têm adiado a realização de um computador quântico útil para o futuro.

A principal das dificuldades é a alta incidência de erros. Entre as causas dos erros está o próprio ambiente: a influência do meio sobre o computador quântico pode levar a erros que podem causar incoerência no sistema, invalidando toda a computação. Além disso, uma outra dificuldade é, ironicamente, a implicação de um dos princípios da Mecânica Quântica que tornam a Computação Quântica interessante em primeiro lugar. A Física Quântica afirma que o ato de medir ou observar um sistema quântico destrói a superposição de estados. Isso quer dizer que, se for feita uma leitura dos dados durante a execução de programa em um computador quântico, todo o processamento será perdido. Assim, a maior dificuldade é conseguir corrigir um erro sem de fato medir o sistema.

Diante dessa situação, programas simuladores de operações de computação quântica têm surgido como ferramentas bastante úteis no estudo e no desenvolvimento de tal ciência (DEUTSH, 1985). Como exemplo, um simulador de circuitos quânticos permite descrever (textualmente e/ou graficamente) um algoritmo quântico em termos de portas e circuitos e testar esse algoritmo para um estado quântico específico através da simulação do hardware assim descrito. A simulação computacional permite o estudo de problemas científicos, a partir da análise dos fenômenos, desenvolvimento de modelos matemáticos para sua descrição e elaboração de códigos computacionais para obtenção daquelas soluções.

Na próxima seção, apresentaremos o simulador de circuitos quânticos desenvolvido durante um projeto PIBICT, no Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande, no ano de 2012. Tal simulador foi montado utilizando-se a linguagem de programação Java e pode servir como instrumento de pesquisa e ensino no tema.

4 O simulador de computação quântica

Em computação quântica, utilizam-se estados quânticos em vez de estados clássicos. O bit é, então, substituído pelo bit quântico, o qubit , e os valores 0 e 1 de um bit são substituídos pelos vetores $|0\rangle$ e $|1\rangle$, conhecida por notação de Dirac, e representados por:

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

A diferença entre um bit e um qubit é que um qubit genérico $|\psi\rangle$ pode também ser uma combinação linear dos vetores $|0\rangle$ e $|1\rangle$, como escrito abaixo:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

Com α e β sendo números complexos.

Dessa forma, a interpretação física do qubit é que ele está simultaneamente nos estados $|0\rangle$ e $|1\rangle$. Isso faz com que a quantidade de informação que pode ser armazenada no estado $|\psi\rangle$ seja infinita.

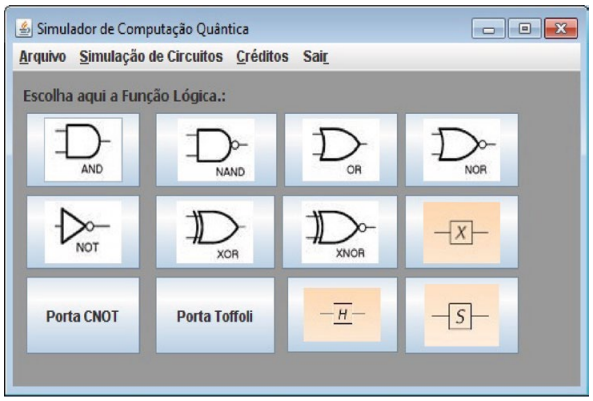
Um simulador de circuitos quânticos é um elemento valioso no ensino e na aprendizagem da Computação Quântica e da Informação Quântica devido à facilidade de uso, a precisão e a velocidade de resposta que tal ferramenta proporciona com relação a cálculos manuais, que é, em geral, a única alternativa disponível.

Apresentamos um breve relato sobre a implementação e concepção do Simulador de Circuitos Lógicos e Quânticos desenvolvido em linguagem

de programação Java. O Simulador deve permitir a edição e simulação de circuitos lógicos e quânticos, sendo assim uma ferramenta de grande valor para estudantes e pesquisadores de Computação Quântica e da Informação Quântica.

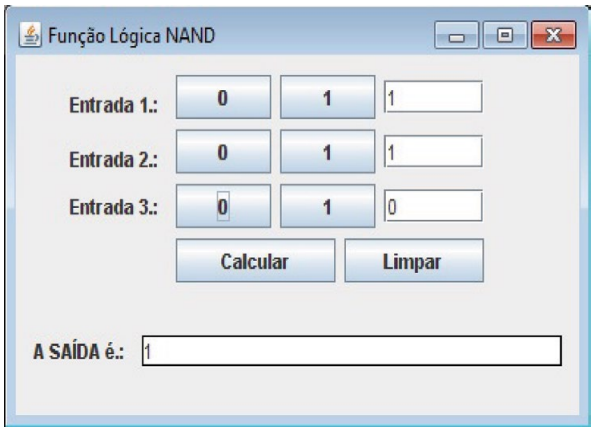
O simulador desenvolvido no nosso projeto contempla tanto portas lógicas clássicas como quânticas. Na Figura 1 temos a interface gráfica do Simulador, ainda em processo de organização do design, mas com todos os botões em perfeito funcionamento. Inicialmente foi desenvolvida a simulação das portas lógicas clássicas: And, Nand, Or, Nor, Not, Xor e Xnor.

Figura 1 – Simulador de Computação Quântica



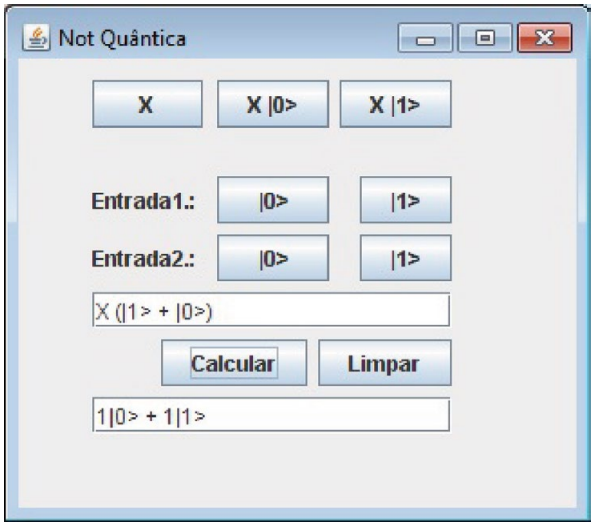
Na Figura 2 evidenciamos o funcionamento da Função Lógica clássica Nand, com até três entradas, de modo que o usuário escolha os valores de entrada e, ao clicar no botão "calcular" o software mostra em seu visor a saída esperada.

Figura 2 – Simulando Circuitos Lógicos



Na Figura 3, evidenciamos o funcionamento da Porta Lógica Not Quântica, com até duas entradas e com seus bits de controle, de modo que o usuário escolha os valores de entrada e, ao clicar no botão "calcular" o software mostra em seu visor a saída esperada. Nesta etapa o usuário pode observar no visor como está ficando o modelo e editar à sua vontade, formando a equação que desejar.

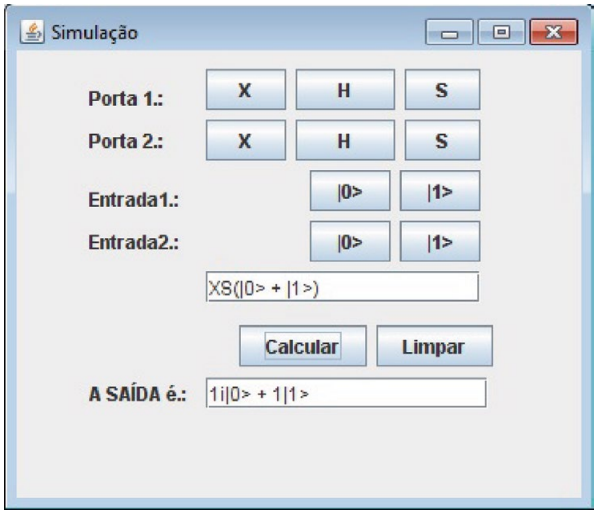
Figura 3 – Simulando Portas Lógicas Quânticas



Com relação às portas lógicas quânticas, o Simulador cobre as versões quânticas das portas lógicas Not, Tofffoli, Cnot, Hadamard e Porta de Fase S. O simulador aborda, também, a simulação à interação entre tais portas lógicas. Tal opção pode ser encontrada na aba de Simulações de Circuitos, localizada na tela inicial do aplicativo.

Na Figura 4, ratificamos a efetividade do componente principal do software, que está na simulação dos circuitos quânticos já elencados nesse trabalho, em que o usuário escolhe, edita e simula circuitos quânticos compostos por até duas portas lógicas, escolhendo as portas e também o valor de suas respectivas entradas..

Figura 4 – Simulando Circuitos Quânticos



Dessa forma, o simulador desenvolvido durante este projeto oferece recursos funcionais que permitem testar portas lógicas clássicas e quânticas, assim como circuitos clássicos e quânticos simples.

5 Conclusões

Neste trabalho, foi planejado e implementado o Simulador de Circuitos Lógicos Quânticos. Em relação à montagem de tais circuitos, o programa oferece recursos de manipulação que permitem ao usuário edição e montagem de circuitos de maneira fácil e intuitiva, usufruindo de uma interface gráfica agradável e com linguagem em Português.

Outra contribuição importante da construção do Simulador é o auxilio que o mesmo deverá dar no ensino e aprendizagem da Computação Quântica fornecendo uma maneira de se testar rapidamente os conhecimentos aprendidos quanto ao estudo de circuitos lógicos e quânticos.

Esperamos, no futuro, equipar o simulador com ferramentas suficientes para que circuitos quânticos mais complexos possam ser abordados. Com isso, também esperamos utilizar tal simulador para reproduzir os algoritmos quânticos mais conhecidos como os de Shor (RUSSEL, 2001) e Grover (SHOR, 1994).

REFERÊNCIAS

BARBOSA, A.A. **Simulação simbólica de circuitos quânticos**, dissertação de mestrado, UFCG, 2008.

BENIOFF, P., **The computer as a physical system: a microscopic quantum mechanical**