Mecânica Quântica: da Física para a Computação

Samuel S. Feitosa[1], **Camila L. Nogueira**[1], **Juliana K. Vizzotto**[1]

[1]Universidade Federal de Santa Maria (UFSM)
Cidade Universitária – 97.105-900 – Santa Maria – RS – Brazil

{sfeitosa,cnogueira,juvizzotto}@inf.ufsm.br

Resumo. *O interesse desta pesquisa é apresentar uma visão de alto nível a respeito da computação quântica para que os leitores possam ter contato com esta recente área. Além disso pode servir de apoio a pesquisadores iniciantes que objetivam buscar referências, no âmbito de iniciar seus estudos nesta área. Deste modo são apresentadas brevemente as origens, principais conceitos e características referentes a computação quântica, sempre que possível fazendo analogia a computação clássica, bem como a atual realidade do hardware quântico.*

Palavras-chave: *Computação quântica, programação quântica, hardware quântico.*

1. Introdução

A computação quântica, primeiramente pensada por Feynman [Feynman 1982], é um campo da teoria da computação que tenta encontrar o que pode ser computado, levando em consideração os princípios da mecânica quântica [Nielsen and Chuang 2011]. Essencialmente, computação clássica pode ser resumida em como tarefas de processamento de informações podem ser codificadas através de um sistema físico clássico, regido pelas leis aplicadas às partículas em escala macroscópica [Vizzotto 2013]. Deste modo a computação quântica pode ser vista como a tarefa de processar informações codificadas em um sistema físico quântico, definido pelo comportamento das partículas em escala microscópica [Williams 2008].

A principal motivação para a pesquisa de outros mecanismos de processamento de informação, é o limite atingido pelos computadores desenvolvidos através do sistema físico clássico. A *Lei de Moore* [Moore 1965] - que diz que o poder computacional dobra aproximadamente a cada dois anos - está deixando de ser válida devido a miniaturização dos componentes dos processadores [Mack 2011], que estão se aproximando de uma escala quântica. Atualmente, os chips de processadores mais poderosos apresentam transistores com aproximadamente 20 nanômetros e de acordo com a *Lei de Moore* rapidamente um transistor chegará ao tamanho de um único átomo. Com componentes em escala microscópica fica praticamente impossível controlar as correntes elétricas que são transmitidas no transistor. Para imaginar o tamanho físico de um transistor, pode-se compará-lo a medidas conhecidas, onde os transistores atuais podem chegar a um tamanho mil vezes menor do que o diâmetro de um fio de cabelo humano.

Deste modo se faz necessário pensar em novos paradigmas para obter capacidades de processamento superiores. A aplicação dos princípios da mecânica quântica fornecem uma perspectiva diferente para o poder de processamento na computação. Utilizando as propriedades microscópicas e seus efeitos, é possível ter, em alguns casos, até

um aumento exponencial no processamento de informações. Explorar estas capacidades através de algoritmos quânticos já propostos poderia impactar na quebra dos mecanismos de criptografia atualmente utilizados [Shor 1994], melhoria no desempenho nas consultas em bases de dados não estruturadas [Grover 1996], etc.

Apesar desta expectativa, esforços para construir sistemas de processamento de informação quântica têm resultado em um sucesso modesto até agora [Yanofsky and Mannucci 2008]. Muito deste trabalho está guardado em centros de pesquisa, onde físicos e engenheiros tem tentado entender e desenvolver técnicas para realizar tal feito. Uma empresa canadense, chamada *D-Wave Systems*, vêm há alguns anos realizando demonstrações do equipamento por eles desenvolvido, e tem sido considerado por muitos o primeiro computador quântico comercial.

Alguns pesquisadores acreditam que o ganho computacional na computação quântica é tão significante, que nenhum progresso concebível na computação clássica estaria apta a superar o poder do processamento da informação quântica [Nielsen and Chuang 2011]. Sabe-se que a computação clássica possui categorias de problemas que não podem ser resolvidos de forma eficiente. Em alguns estudos teóricos, foi demonstrado que através do uso da computação quântica, é possível resolver problemas que teriam uma solução eficiente impossível na computação atual [Gruska 2000].

O artigo está organizado da seguinte forma: na seção 2 é apresentada uma visão histórica com relação as descobertas no campo de computação quântica. O capítulo 3, introduz os principais conceitos para iniciar os estudos nesta área, considerando *qubits* e operações quânticas, um *framework* para descrever algoritmos quânticos e as características que possibilitam o ganho computacional dos computadores quânticos. O capítulo 4 lista algumas pesquisas relacionadas ao *hardware* quântico, bem como apresenta brevemente o computador *D-Wave*. Ao final, são apresentadas algumas considerações finais, e diversas referências que possibilitam o aprofundamento dos estudos nesta área.

2. Histórico

Há quase um século da descoberta da mecânica quântica, mais de meio século da invenção da teoria da informação e da chegada da computação digital, que pesquisadores perceberam que a física quântica pode alterar profundamente as características do processamento de informações.

A primeira vez que pensou-se em utilizar física quântica na computação foi em 1981, onde Richard Feynman sugeriu que somente através da Computação Quântica seria possível simular com eficiência os efeitos da natureza [Feynman 1982]. Então Feynman propôs um modelo básico de um computador quântico que seria capaz de realizar tais simulações. Em 1985, David Deutsch apresentou em seu artigo [Deutsch 1985] que um computador universal quântico pode executar processos que a máquina de Turing não poderia, incluindo a capacidade de gerar números genuinamente randômicos, executar alguns cálculos paralelos em um único registrador, entre outros. Em 1989, ele descreveu um segundo modelo de computação quântica: o circuito quântico [Deutsch 1989]. Neste esforço, ele demonstrou que circuitos quânticos podem realizar qualquer computação clássica e também computar as mesmas informações passíveis de execução na descrição

do computador universal quântico. Além disso, Deutsch foi o primeiro a conceber um algoritmo quântico, que utilizaria os conceitos do paralelismo quântico, sendo capaz de responder se uma função é balanceada ou constante.

Nas últimas décadas também foi obtido certo progresso no desenvolvimento experimental de um computador quântico. O contexto para o desenvolvimento deste computador foi aprimorado. Um computador quântico não será uma versão mais rápida, maior ou menor que um atual. Ao invés disso, será um tipo diferente de máquina, construída para controlar coerentemente ondas de mecânica quântica para diferentes aplicações [T. D. Ladd and O'Brien 2010].

Este primeiro passo dado por Deutsch culminou em várias pesquisas na área de computação quântica, sendo demonstrado por Peter Shor em 1994 a resolução de outros importantes problemas da computação clássica, o problema de encontrar os fatores primos de um inteiro e o então chamado "logaritmo discreto" [Shor 1994], que poderiam ser resolvidos de forma eficiente por computadores quânticos. O trabalho de Shor desencadeou várias pesquisas nesta área, incluindo os campos da computação, informação e complexidade quântica. Em 1995, outro nome importante no cenário surgiu, Lov Grover mostrou que pesquisas em espaços de busca não estruturados também podem ser melhoradas por um computador quântico [Grover 1996].

Ainda são incertas as aplicações exatas de um computador quântico. Já foi demonstrado que é possível resolver de forma mais eficiente problemas clássicos, porém, não é possível afirmar que um computador quântico será sempre mais rápido que um computador clássico. A computação clássica, apesar de também ser recente, possui vários campos de estudo, e o projeto de algoritmos já é bem conhecido. Na computação quântica, o projeto de algoritmos é difícil, pois os projetistas deparam-se com a intuição clássica que está enraizada desde o início do aprendizado sobre a computação e também, que não basta apenas escrever um algoritmo quântico, este tem de ser melhor dos que os clássicos já apresentados [Shor 2004].

3. Computação Quântica

O início do século XX deflagrou uma revolução no campo da física. Muitas das teorias até então propostas apresentaram divergências com a possibilidade de investigação através de escalas microscópicas. Os físicos do século XX - que hoje são chamados de físicos clássicos - não conseguiam compreender as propriedades e características nestas escalas, que mais tarde foram estudadas e nomeadas como física quântica, ou como tem sido chamada, física moderna.

A física clássica é aquela que estuda as partículas e suas reações em escalas macroscópicas. Há séculos que existem teorias e modelos matemáticos que descrevem o comportamento dessas partículas. A partir do avanço tecnológico e da possibilidade de estudo de partículas em escalas menores, foram aplicados os modelos físicos já conhecidos e foi percebido que essas partículas não se comportavam conforme o previsto. Mesmo Albert Einstein não conseguiu compreender totalmente os efeitos apresentados pela mecânica quântica [Nielsen and Chuang 2011].

Ao estudar os conceitos de física quântica, depara-se com o efeito da dualidade onda partícula, característica que é extremamente importante para computação quântica.

Primeiramente, é necessário conceituar ambas as coisas. Uma onda pode ser vista como uma perturbação que se propaga por um meio com características de frequência, comprimento de onda, amplitude, espalhamento no espaço e são passíveis de interferência. Já uma partícula pode ser vista como algo que se move no espaço e que em condições normais, é indivisível e tem uma trajetória bem definida. Em escala macroscópica, os objetos ou coisas podem ser descritos apenas como onda ou como partícula [Vizzotto 2013].

Objetos em escala microscópica podem possuir propriedades de onda e partícula ao mesmo tempo, tal característica foi provada através do experimento da dupla fenda, onde é lançado um único fóton - uma partícula elementar que é um ingrediente básico da luz - e analisado o seu comportamento através de sua passagem por duas fendas paralelas. É percebido que, o fóton ao passar pelas duas fendas, reflete em lugares diferentes após sua passagem, apresentando características de ondas. Porém, ao fechar uma das fendas, o efeito é diferente, e a reflexão apresenta característica de partículas.

Essas propriedades percebidas em escala microscópica fornecem uma possibilidade diferente das partículas macroscópicas, a possibilidade da *superposição de estados*. A superposição de estados é a capacidade de uma partícula microscópica apresentar todos os seus estados distintos de maneira simultânea e representa o fundamento principal da mecânica quântica. Esta capacidade especial é o que permite o chamado paralelismo quântico, que será apresentado posteriormente.

3.1. Qubits e Operações Quânticas

A unidade básica de informação na computação clássica é o *bit* tradicional, que representa o sistema físico clássico binário, sendo capaz de representar apenas dois estados (*true* ou *false*, 0 ou 1). Qualquer informação é descrita como uma combinação de sequências de *bits*.

Na computação quântica, a menor partícula de informação é chamada de *quantum bit* ou *qubit*. O *qubit* apresentam uma diferença essencial se comparado com o *bit*, pois ele não está restrito aos dois estados básicos do *bit* clássico, podendo estar efetivamente em ambos os estados (0 e 1) ao mesmo tempo [Nielsen and Chuang 2011]. Vários centros de pesquisa tem estudado maneiras de manipular partículas que sejam capazes de fornecer as características quânticas, porém, ainda existem diversos desafios na manipulação física de elementos em escala microscópica [Mermin 2007].

O campo de estudo teórico da Mecânica Quântica, define matematicamente um *qubit* como sendo um vetor, onde cada uma de suas posições armazena a *amplitude de probabilidade* α e β de cada um dos estados básicos. As amplitudes de probabilidade são representadas como *números complexos*, onde $|\alpha|^2 + |\beta|^2 = 1$ [Yanofsky and Mannucci 2008].

Intuitivamente, pode-se visualizar um *qubit* como sendo 0, 1 ou ambos os estados simultaneamente, tendo um coeficiente numérico que determina a probabilidade de cada estado puro. Na expressão 1 percebe-se que $|\alpha|^2$ representa a probabilidade do *qubit* estar no estado $|0\rangle$ e $|\beta|^2$ representa a possibilidade do *qubit* estar no estado $|1\rangle$.

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1}$$

Para descrever os estados quânticos puros $|0\rangle$ e $|1\rangle$, o número 0 representa a probabilidade nula e o número 1 representa 100% da probabilidade de ocorrência de determinado estado. Então, na expressão 2 percebe-se que para o estado quântico $|0\rangle$ a amplitude de probabilidade α está definida como 1 e β está definido como 0, representando 100% para obtenção do valor 0. O mesmo ocorre de maneira similar para representar o estado quântico $|1\rangle$.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

Embora α e β sejam representados por números complexos, para muitos propósitos não existe muita perda em imaginá-los como números reais [Nielsen and Chuang 2011]. As amplitudes de probabilidade proveem o significado físico para a função de onda, ou em outras palavras, representam a superposição dos estados quânticos.

Qualquer outro estado com valores diferentes para α e β representa uma *superposição quântica* de $|0\rangle$ e $|1\rangle$, conforme apresentado na expressão 3.

$$|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \qquad |-\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} \tag{3}$$

Os estados $|+\rangle$ e $|-\rangle$ são muito utilizados e representam a obtenção de $|0\rangle$ com 50% de probabilidade e $|1\rangle$ com 50% de probabilidade. Estes estados em *superposição* fornecem a computação quântica uma característica chamada *paralelismo quântico*. Essencialmente, devido à *superposição* de estados, um *qubit* pode assumir os valores 0 e 1 ao mesmo tempo. Esta propriedade é explorada nos algoritmos quânticos, possibilita a obtenção de ganho exponencial pela possibilidade de manipular várias possibilidades em paralelo.

Na tabela 1 são apresentados como o espaço de estados do *qubit* cresce com o número de *qubits*. Pode-se verificar que, a cada *qubit* adicionado, dobra-se a capacidade de representar informação em um nível quântico.

Tabela 1. Espaço de estados do *qubit*.

# qubits	possibilidades	potência
1	0 ou 1	2
2	00,01,10,11	4
3	000,001,010,011,100,101,110,111	8
N		2^N

Os *bits* clássicos podem ser examinados para determinar seu valor atual (0 ou 1), e isto é feito a todo momento nos computadores, manipulando o conteúdo da memória. No caso dos *qubits* é impossível visualizar seus valores para determinar seu estado atual (amplitudes α e β) sem interferir com o sistema. Uma leitura ao estado quântico realiza uma *operação de medida*.

Na computação quântica pode-se efetuar dois tipos de operações: *operações de medida* e *transformações unitárias*. A operação de medida está relacionada à maneira de obter informações de um estado quântico. Transformações unitárias referem-se a operações que transformam o atual estado quântico em outro, como ocorre na aplicação de uma função na computação clássica.

A computação quântica difere da computação clássica por ser probabilística e não determinística, ou seja, a operação de medida trabalha sobre as amplitudes de probabilidade de um estado quântico. Quando uma medição é executada, acontece um colapso nas amplitudes de probabilidades e apenas um dos estados básicos é retornado, como $|0\rangle$ ou $|1\rangle$. Em outras palavras, após uma medição, o *qubit* fica em um estado conhecido, e as amplitudes de probabilidade são destruídas. A operação de medida é utilizada para obter as informações após o processamento de um algoritmo quântico.

De forma similar ao modo de processar informações em sistemas clássicos, na computação quântica um algoritmo é projetado como uma série de aplicações de transformações unitárias, ou *portas quânticas*. Estas portas aplicadas aos *qubits* modificam seus valores de modo a transformar um estado quântico inicial na saída desejada.

Os algoritmos quânticos são descritos através de um conjunto finito de instruções ordenadas e não ambíguas, executando em um computador quântico, fazendo uso de diversas propriedades específicas como superposição e emaranhamento quântico [Williams 2008]. Todo algoritmo quântico trabalha sobre o seguinte *framework* básico [Yanofsky and Mannucci 2008].

1. Iniciar com um conjunto de *qubits* em seus estados básicos.
2. Colocar todos os *qubits* em superposição.
3. Aplicar uma série de transformações unitárias para resolver o problema em paralelo.
4. Realizar a operação de medida sobre os *qubits*.

Embora possa ter algumas variações, o processo dos algoritmos quânticos tem por objetivo explorar ao máximo a capacidade de processamento (paralelismo) e de comunicação (emaranhamento).

3.2. Características dos Estados Quânticos

O modelo de computação quântica tem o objetivo de aplicar as leis que regem o funcionamento das partículas na mecânica quântica, aproveitando-se de características como *emaranhamento* e *superposição* de estados, fornecendo capacidades de comunicação e processamento de informação muito superiores comparadas com a computação atual [Simon 1994].

Emaranhamento é um fenômeno fundamental na computação quântica. Resumidamente, um par de *qubits* em um estado quântico é dito *emaranhado* se ele não puder ser expresso através do produto tensorial de *qubits* individuais. É um elemento chave nos efeitos como teleportação e distribuição de chaves quântica, algoritmos quânticos e correções de erros, sendo de grande utilidade na computação e informação quântica, apesar de suas características ainda não serem totalmente compreendidas pelos pesquisadores [Nielsen and Chuang 2011].

Neste fenômeno da mecânica quântica, no qual os estados quânticos de dois ou mais objetos são descritos como referência entre eles, mesmo que os objetos individuais estejam separados no espaço, é possível preparar duas partículas em um estado quântico único, de modo que quando um deles é observado, o outro sempre será influenciado por esta medição, não importando a distância entre eles.

No ponto de vista computacional, o *emaranhamento* tem um papel central na teoria da informação quântica, sendo capaz de interconectar duas partes fisicamente distantes, não permitindo a sua cópia, sem possibilitar a interceptação da informação, além de auxiliar na melhoria de performance dos algoritmos quânticos. É uma das principais razões da computação quântica não poder ser simulada eficientemente por computadores clássicos [Gruska 2000].

A *superposição de estados* oferece à computação quântica uma importante propriedade que é seu diferencial, o *paralelismo quântico*. O estado de superposição permite ao *qubit* armazenar ao mesmo tempo mais de um valor. Por exemplo, um *qubit* pode armazenar 0 e 1 com uma superposição coerente desses estados através de suas amplitudes de probabilidade, como mostrado anteriormente. Devido a essa propriedade a computação quântica promete causar uma revolução na maneira de tratar problemas normalmente intratáveis de forma eficiente na computação clássica.

De modo simplificado o paralelismo quântico permite aos computadores quânticos avaliarem uma função $f(x)$ para muitos valores diferentes de x simultaneamente [Nielsen and Chuang 2011]. Geralmente, a computação de uma função f é determinada por uma *operação unitária* que age sobre dois ou mais *qubits*, sendo que, na maioria dos casos, os primeiros representam os dados de entrada para a função, e o último sendo utilizado para armazenar a própria função e permitir a simultaneidade do processamento.

Deste modo, supondo que a função $f(x) : \{0,1\} \rightarrow \{0,1\}$ mapeia um único bit x para um único bit $f(x)$. Para computar esta função é conveniente considerar um computador quântico de dois *qubits* que começa no estado $|x, y\rangle$ e com um sequência apropriada de portas lógicas este estado pode ser transformado em $|x, y \oplus f(x)\rangle$. Esta transformação pode ser definida como:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle \tag{4}$$

Na figura 1 é apresentada a transformação unitária que trabalha com 2 *qubits* de entrada, sendo $x = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $y = |0\rangle$ [Nielsen and Chuang 2011].

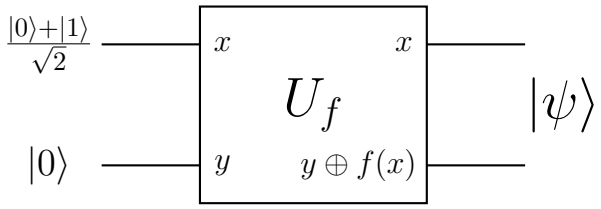

Figura 1. Transformação unitária para avaliar $f(0)$ e $f(1)$ simultaneamente.

Ao aplicar a transformação unitária aos *qubits* mostrados o seguinte estado é ob-

tido:

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \tag{5}$$

Deste modo transformação unitária U_f realiza a invocação da função f sobre todos valores em uma única avaliação de U_f, executando $f(0)$ e $f(1)$ simultaneamente. Caso fossem passados mais de 2 *qubits* para esta transformação unitária o mesmo ocorreria. Poder calcular todas as possibilidades da função f ao mesmo tempo é o que caracteriza o *paralelismo quântico*. É importante notar que após a realização do processamento das entradas ainda é preciso realizar operações para interpretar o resultado. Para tal resultado é necessária a elaboração de algoritmos quânticos que aproveitem as possibilidades deste paralelismo [de Lima and Júnior 2007].

4. Estado Atual do Hardware Quântico

Nos últimos anos, pesquisadores puderam comprovar que as propriedades da mecânica quântica aplicadas em seus algoritmos quânticos podem prover melhorias de performance perante a computação clássica. Atualmente muitos grupos de pesquisa tem trabalhado para construir o computador quântico, o qual pode aumentar drasticamente o poder de computação de determinadas tarefas. Entretanto, parece incerto qual componente físico será capaz de ser manipulado com sucesso para permitir a manipulação de características quânticas [T. D. Ladd and O'Brien 2010].

Uma questão central para o desenvolvimento de *hardware* quântico é: que forma ele terá e como manipulá-lo efetivamente? não existem respostas simples para isto. A construção de bits quânticos geralmente é imaginada a partir de pequenas formas de matéria, com um átomo isolado em uma armadilha de íons, mas também podem ser construídos a partir de componentes eletrônicos maiores, como em alguns sistemas supercondutores [Aaronson 2008].

Quando se pensa na construção de hardware quântico, um mínimo de requisitos se faz necessário: o hardware deve permanecer isolado do meio externo, pois qualquer influência mínima no sistema causa incoerência nos resultados, embora algumas técnicas para correção de erros quânticos têm sido desenvolvidas para amenizar esta situação. Além disso, um sistema quântico deve ter capacidade de crescer (escalabilidade) e possuir uma série de operações lógicas de controle. O desafio de construir um computador quântico está em manter todos esses requisitos simultaneamente, conseguindo controlar o sistema, medir seus resultados e preservar o forte isolamento de suas partes do restante do ambiente [DiVincenzo 2000].

Diferentes estratégias e componentes físicos tem sido utilizadas para atingir este objetivo, dentre as principais estão a utilização de fótons, átomos aprisionados, ressonância magnética nuclear, supercondutores, entre outras abordagens. Na maioria dos casos o principal problema é conseguir manter as propriedades quânticas na utilização de muitos *qubits* [T. D. Ladd and O'Brien 2010].

Além dos centros de pesquisa em computação quântica, existe a empresa *D-Wave Systems*, que apresentou um controverso computador quântico, o qual vem sendo experimentado por grupos de pesquisas e grandes empresas.

4.1. D-Wave

O problema da falta de reconhecimento está desaparecendo para a *D-Wave Systems*, a primeira e até então única empresa a construir computadores quânticos. Após ter sido inicialmente desacreditada e ridicularizada pela comunidade de pesquisa, a empresa passou a ser levada mais a sério, tanto que as gigantes *Lockheed Martin* e *Google* compraram seus exemplares do computador quântico *D-Wave*, com preço especulado de mais de 10 milhões de dólares [Jones 2013a].

Este computador, oferecido pela empresa *D-Wave Systems*, localizada próximo a Vancouver, Canadá, tem gerado muita discussão sobre o fato de realmente ser um computador que utiliza propriedades da mecânica quântica e se é, de fato, mais rápido ou melhor que os computadores convencionais. Em resumo, o computador quântico *D-Wave* mostrou-se milhares de vezes mais rápido do que outros computadores comerciais para resolver um problema muito específico para o qual ele foi projetado. Para outros tipos de problemas, ele manteve a média de tempo de outros computadores e ainda não se sabe se ele terá melhoria de velocidade de processamento quando ele possuir um processador com maior quantidade de *qubits* [Jones 2013b].

A comparação do computador *D-Wave* com os computadores convencionais não é algo trivial, uma vez que ele opera de modo diferente, não apenas pelas questões dos bits quânticos, mas também por que ele não utiliza portas lógicas para executar operações. Ao invés disso, ele utiliza algo chamado de "*annealing*", através do modelo de programação "*adiabático*" [Boixo et al. 2014].

A empresa *D-Wave System* foi fundada em 1999, e vem a cada ano apresentando novas versões de seu processador quântico. O crescimento do número de *qubits* tem sido, aproximadamente, dobrado a cada ano, o que tem superado a velocidade de crescimento predita pela lei de Moore. O computador comprado pela *Lookheed Martin*, chamado de *D-Wave One* possuia 128 *qubits*, em 2011. Em 2013, uma parceria firmada entre o *Google* e a *NASA* possibilitou a aquisição do *D-Wave Two*, composto por 512 *quits* [Jones 2013a].

Muitas publicações relacionadas aos resultados da utilização do *D-Wave* tem sido apresentadas, onde pode-se citar a utilização do processador quântico com mais de cem *qubits* [Boixo et al. 2014], aprendizagem de máquina através da programação quântica adiabática [Pudenz and Lidar 2011], apresentação de emaranhamento quântico [Lanting et al. 2014], etc.

5. Considerações Finais

Neste artigo foi apresentada uma breve introdução a respeito dos fundamentos da computação quântica, desde os primeiros pensamentos com relação a aplicação da mecânica quântica na computação, alguns aspectos das partículas físicas em escala microscópica, adentrando num comparativo entre os fundamentos da computação clássica com a computação quântica. Foram apresentados também os principais conceitos que são utilizados para o desenvolvimento de algoritmos quânticos. Após isto, foram sumarizadas as tentativas de construção de hardware para esta área, juntamente com uma apresentação do primeiro computador quântico comercial.

Este material tem a intenção de facilitar o início dos estudos neste campo de pesquisa, pois existem muitas áreas envolvidas, e muitas fontes, tornando o início do processo

de aprendizado um tanto temeroso.

Com este estudo, foi possível perceber que, de fato, houve bastante avanço na área de computação quântica, e que os pesquisadores estão realmente interessados em explorar o potencial da computação quântica para resolução de problemas que não tem soluções eficientes na computação clássica. Também foi explorado o fato da computação clássica estar próxima ao limite físico do desenvolvimento de componentes, o que, em curto prazo esgotará a capacidade de crescimento do poder de processamento dos computadores atuais.

Além disso, também foi possível perceber que há vários centros de pesquisa investindo no desenvolvimento de computadores quânticos com componentes físicos dos mais variados e ainda não existe uma definição da melhor tecnologia para construir esses processadores. Por outro lado, na área de software, está sendo preferido trabalhar com modelos de circuitos quânticos, apesar do computador *D-Wave* implementar um modo diferente de programação.

Referências

Aaronson, S. (2008). The limits of quantum computers. *Nature Physics*, 298,online.

Boixo, S., Rønnow, T. F., Isakov, S. V., Wang, Z., Wecker, D., Lidar, D. A., Martinis, J. M., and Troyer, M. (2014). Evidence for quantum annealing with more than one hundred qubits. *Nature Physics*, 10:218–224.

de Lima, A. F. and Júnior, B. L. (2007). *Computação Quântica: noções básicas utilizando a linguagem de circuitos quânticos*. Editora da Universidade Federal de Campina Grande, 1st edition.

Deutsch, D. (1985). Quantum theory, the church-turing principle and the universal quantum computer.

Deutsch, D. (1989). Quantum computational networks. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 425(1868):73–90.

DiVincenzo, D. P. (2000). Quantum computers. *arXiv*.

Feynman, R. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proc. 28., Annual ACM Symposium on Theory of Computing*, pages 212–219.

Gruska, J. (2000). *Quantum Computing*. Mcgraw Hill Book.

Jones, N. (2013a). Computing: The quantum company. http://www.nature.com/news/computing-the-quantum-company-1.13212.

Jones, N. (2013b). Quantum computer passes speed test. http://blogs.nature.com/news/2013/05/quantum-computer-passes-speed-test.html.

Lanting, T., Przybysz, A. J., Smirnov, A. Y., Spedalieri, F. M., Amin, M. H., Berkley, A. J., Harris, R., Altomare, F., Boixo, S., Bunyk, P., Dickson, N., Enderud, C., Hilton, J. P., Hoskinson, E., Johnson, M. W., Ladizinsky, E., Ladizinsky, N., Neufeld, R., Oh, T., Perminov, I., Rich, C., Thom, M. C., Tolkacheva, E., Uchaikin, S., Wilson, A. B.,

and Rose, G. (2014). Entanglement in a quantum annealing processor. *Phys. Rev. X*, 4:021041.

Mack, C. (2011). Fifty years of moore's law. *Semiconductor Manufacturing, IEEE Transactions on*, 24(2):202–207.

Mermin, N. D. (2007). *Quantum Computer Science: An Introduction*. Cambridge University Press, New York, USA.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Eletronics*, 8/38/online.

Nielsen, M. A. and Chuang, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition.

Pudenz, K. and Lidar, D. (2011). Quantum adiabatic machine learning. *arXiv*.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. IEEE Symposium on Foundations of Computer Science*, pages 124–134.

Shor, P. W. (2004). Progress in quantum algoritms.

Simon, D. R. (1994). On the power of quantum computation. *SIAM Journal on Computing*, 26:116–123.

T. D. Ladd, F. Jelezko, R. L. Y. N. C. M. and O'Brien, J. L. (2010). Quantum computers. *Nature Physics*, 464/online.

Vizzotto, J. K. (2013). Quantum computing: State-of-art and challenges. In *II Workshop-School on Theoretical Computer Science*, DLSC,RS.

Williams, C. P. (2008). *Explorations in Quantum Computing*. Springer Publishing Company, Incorporated, 2nd edition.

Yanofsky, N. S. and Mannucci, M. A. (2008). *Quantum Computing for Computer Scientists*. Cambridge University Press.