DECIFRANDO A COMPUTAÇÃO QUÂNTICA

DECIPHERING THE QUANTUM COMPUTING

Felipe Mattielo[1], Gesiel Gomes Silva[2], Ronni Geraldo Gomes de Amorim[3], Washington Barbosa da Silva[4]

[1]*Instituto Federal de Educação, Ciência e Tecnologia de Goiás/Campus Luziânia /Técnico Integrado em Mecânica, ofelipedbzgt@hotmail.com*

[2]*Instituto Federal de Educação, Ciência e Tecnologia de Goiás/Campus Luziânia /Departamento de Áreas Acadêmicas, gesiel_sax@yahoo.com.br*

[3]*Instituto Federal de Educação, Ciência e Tecnologia de Goiás/Campus Luziânia /Departamento de Áreas Acadêmicas, ronniamorim@gmail.com*

[4]*Universidade de Brasília (UnB) – Instituto de Física, Física Atômica e Molecular*

plutaow@yahoo.com.br

Apresentamos neste trabalho uma revisão bibliográfica sobre Computação Quântica. Discutimos questões fundamentais que justificam o investimento em pesquisas nesta área da ciência, bem como apresentamos as perspectivas de suas aplicações. O principal diferencial deste trabalho é o seu caráter pedagógico, direcionado a um público abrangente, que não necessariamente tenha conhecimentos prévios sobre mecânica quântica.
Palavras-chave: mecânica quântica, ciência da computação, computação quântica, *q-bit*.

We present in this work a literature review about Quantum Computing. We discuss fundamental issues that justify investment in research in this area of science, as well as we present perspectives of their applications. The main distinguishing feature of this work is its pedagogical content, directed to a large audience, which does not necessarily have previous knowledge of quantum mechanics.
Key-words: quantum mechanics, computing science, quantum computing, *q-bit.*

INTRODUÇÃO

No século XX, a humanidade acompanhou um virtuoso desenvolvimento tecnológico, que se refletiu nas mais diversas áreas de conhecimento e setores de atividades. Um fato que muitas pessoas desconhecem é que o grande salto tecnológico dado pelo homem no século passado se apoiou nos dois grandes triunfos intelectuais estabelecidos no mesmo período. As duas grandes dádivas científicas que precederam as descobertas tecnológicas que modificaram o estilo de vida do homem são a Mecânica Quântica e a Ciência da Computação. Se hoje temos computadores cada vez mais velozes e mais potentes, equipamentos eletrônicos que permitem diagnósticos médicos eficazes, dentre muitos outros artefatos eletrônicos que melhoraram nossa qualidade de vida, devemos gratidão a todos os cientistas que de alguma forma contribuíram no desenvolvimento dessas duas áreas do conhecimento.

Por incrível que pareça, a grande revolução mencionada no parágrafo anterior teve início em uma crise que a Física atravessava no fim do século XIX, pois nesse período havia alguns fenômenos naturais que não eram explicados pelas teorias físicas até então existentes. Nesse escopo, existe uma data precisa para o nascimento da Física Quântica, trata-se do dia 14 de dezembro de 1900, quando o cientista Max Planck explica a emissão de radiação do corpo negro. A explicação elaborada por Planck foi baseada na hipótese de que as paredes da cavidade emitiam radiação sempre em pacotes, que deveriam ser múltiplos inteiros de uma determinada quantia mínima, ou seja, a radiação deveria ser quantizada. Alguns anos mais tarde, em 1905, o renomado físico alemão Albert Einstein elucida o Efeito Fotoelétrico, que era outro fenômeno não explicado pela teoria ondulatória da luz. O efeito fotoelétrico consiste na emissão de

elétrons por uma superfície metálica bombardeada por um feixe de luz. Embora muitos de nós não saibamos, tal efeito é bem familiar, pois está presente em nosso cotidiano, como por exemplo, as portas que abrem e fecham automaticamente têm o funcionamento baseado nesse fenômeno. Einstein explicou o efeito fotoelétrico admitindo a hipótese de que a luz é constituída por pacotes concentrados de energia, que atualmente denominamos fótons, e assim, o fenômeno em questão é facilmente explicado quando consideramos a colisão entre os fótons da radiação incidente e os elétrons dos metais. É importante notarmos que os trabalhos de Einstein e Planck sugeriam a quantização, mas não explicavam o porquê. Um problema parecido surgiu quando o físico dinamarquês Niels Bohr, em 1913, introduziu o seu modelo atômico, no qual supôs que o elétron poderia se mover somente em órbitas determinadas onde não emitia radiação eletromagnética. A radiação era emitida somente quando o elétron "saltava" de uma órbita para outra. Com esse modelo, Bohr solucionou a estabilidade atômica e explicou o espectro de radiação discreto para o átomo de hidrogênio, porém, não ficou claro o motivo pelo qual o elétron não poderia ocupar posições intermediárias no espaço. Assim, por meio desses exemplos, percebemos que a teoria quântica desenvolvida até o primeiro quarto do século XX possuía bases teóricas e conceituais frágeis, pois os princípios eram esparsos e os enunciados eram criados com a finalidade específica de atender a uma necessidade pontual. Nesse escopo, os físicos ressentiam-se de postulados autênticos e princípios gerais dos quais poderiam formular uma teoria consistente, eficiente e abrangente. Esse desejo dos físicos se tornou realidade com o surgimento da Mecânica Quântica [1-10].

A Mecânica Quântica é considerada a teoria científica mais bem sucedida da história da ciência. Esse fato se deve à infalibilidade, até o momento, de suas previsões serem constatadas mediante os experimentos. A Mecânica Quântica é a teoria física utilizada para tratar as partículas microscópicas, de ordem de tamanho atômico ou molecular, pois se utilizarmos as leis de Newton para analisarmos o comportamento de partículas com essa ordem de tamanho, chegaríamos a resultados incompatíveis com os experimentos. Sendo assim, a Mecânica Quântica constitui a base da Física Atômica, da Física Nuclear, da Física do Estado Sólido e da Química Moderna, no sentido que não é espantoso que um grande número de utensílios com valor tecnológico agregado tenham seus princípios de funcionamento embasados na Mecânica Quântica. Para se ter uma idéia, desde o pós-guerra, cerca de um terço do produto interno bruto dos Estados Unidos é oriundo da aplicação da Mecânica Quântica [11]. Dessa forma, quando observarmos, por exemplo, os modernos telefones celulares e televisores, além de diversos outros equipamentos eletrônicos, devemos nos lembrar que são oriundos da vasta aplicabilidade da teoria quântica. E ainda, há projeções que indicam que a partir da segunda década do século corrente, boa parte dos empregos em manufatura no mundo estarão ligados à nanotecnologia, e para se trabalhar nessa escala é indispensável um conhecimento sólido em mecânica quântica.

No primeiro parágrafo deste texto mencionamos os dois grandes triunfos intelectuais da humanidade no século XX. Contudo, até o momento tratamos apenas de um deles. Logo, deixaremos a Mecânica Quântica um pouco de lado para enforcarmos a Ciência da Computação. De certa forma, podemos dizer que a ciência da computação nasceu com o notável artigo do matemático inglês Alan Turing em 1936. Naquele trabalho, Turing desenvolveu a noção abstrata do que conhecemos como computador programável, o que ficou conhecido como máquina de Turing. Este importante aparato proposto por Turing opera com seqüências lógicas de unidades de informação chamadas *bits* (*binary*

digit), os quais podem adquirir os valores "0" ou "1". A idéia de Turing foi tão importante para o desenvolvimento da humanidade que os computadores que utilizamos hoje, desde o simples notebook que utilizamos em casa até o mais potente computador de um grande centro de pesquisa, certamente tratam-se de uma realização física da máquina de Turing. Assim, toda a informação fornecida a um computador é lida, processada e retornada sob a forma de seqüências de *bits*. Um fato que revela o poder da máquina de Turing é decorrente da chamada tese de Church-Turing, a qual estabelece que a máquina de Turing, apesar de simples, é capaz de resolver qualquer problema computacional solúvel por qualquer outro tipo de computador. Essa tese implica que se existir algum problema que seja insolúvel para a máquina de Turing, tal problema não poderá ser resolvido por nenhum outro tipo de computador. A tese de Church-Turing diz que não precisamos considerar máquinas diferentes da máquina de Turing para saber se um problema é computável ou não, mas a tese não diz nada sobre o tempo necessário para solucionar um problema que possa ser computável. Isso possibilitou que os computadores evoluíssem em velocidade, mas sem perder o princípio fundamental de funcionamento baseado nos *bits*.

Nesse sentido, conforme veremos neste trabalho, chegará um momento na evolução dos computadores que será inevitável a fusão dos dois trunfos intelectuais citados nesta introdução. Esse grande acontecimento abrirá as portas para o que chamamos de Computação Quântica, que poderá revolucionar a forma atual que a humanidade trata a informação. Sendo assim, o objetivo deste trabalho é apresentar a Computação Quântica de uma forma pedagógica, na perspectiva de sua utilização em escolas da educação básica, bem como na informação do público em geral. Com isso, a estrutura deste texto está organizada da seguinte forma: na seção 2 estudaremos a lei de Moore; na seção 3 trataremos dos *q-bits* e suas propriedades; na seção 4 veremos as vantagens dos algoritmos quânticos; na seção 5 realizaremos uma breve discussão sobre redes neurais; na seção 6 estudaremos sobre o teleporte quântico, além de outra propriedades da mecânica quântica úteis à computação quântica; na seção 7 apresentaremos nossas considerações finais e perspectivas.

A LEI DE MOORE

Há evidências que o primeiro computador programável tenha surgido no ano de 1941, durante a II Guerra Mundial, e sua invenção é atribuída ao engenheiro alemão Konrad Zuse. O computador desenvolvido por Zuse recebeu o nome de Z3 e era inteiramente mecânico, de forma que a informação era processada por meio do movimento das engrenagens. Nesse mesmo período, cientistas da Inglaterra e dos Estados Unidos também trabalhavam em projetos tecnológicos parecidos, e assim desenvolveram dois computadores muito importantes para a evolução da computação, chamados respectivamente de Colossus e ENIAC. A grande evolução desses computadores em relação ao Z3 foi o uso da eletrônica, o que possibilitou um aumento virtuoso na velocidade de processamento, pois correntes e cargas elétricas podem ser manipuladas mais rapidamente que as engrenagens do Z3. No entanto, foi a descoberta dos transistores que possibilitou o desenvolvimento de computadores rústicos como os descritos acima até o que temos hoje. O fato é que o notebook que utilizei para escrever este texto é cerca de dez milhões de vezes mais rápido que o ENIAC e muito mais leve, haja vista que o ENIAC pesava 27 toneladas. Mesmo com relevante diferença na velocidade de processamento e no peso, o meu notebook e o ENIAC utilizam cargas e correntes elétricas para guardar e processar informações [12, 13].

Se analisarmos essa evolução dos computadores utilizando um parâmetro mais eficaz para o nosso propósito, temos que em 1950 eram necessários 10^{19} átomos - isso mesmo, 10 bilhões de bilhões - para representar um único *bit* de informação. Há projeções que indicam que em poucos anos, um *bit* será representado por apenas um átomo. Essas projeções são baseadas no que denominamos de Lei de Moore. Gordon Moore, fundador da empresa norte-americana de microprocessadores Intel, observou, na década de 1960, que o número de átomos necessários para representar um *bit* se reduzia à metade aproximadamente a cada 1 ano e meio. Isto é equivalente a dizer que o número de transistores em um circuito integrado dobra a cada 18 meses, e isso é mostrado no gráfico da figura 1, onde percebe-se a conveniência da previsão feita por Moore para analisarmos o desenvolvimento dos computadores. Como um exemplo, podemos citar o processador 8086 da Intel que em 1978 tinha 29 mil transistores, enquanto o Pentium IV, lançado em 2000, já tinha 42 milhões. O processador do laptop que utilizo no meu dia a dia tem praticamente 1 bilhão de transistores! O leitor mais experiente notará que assistiu parte dessa evolução de camarote, e sempre comemorando cada etapa desse desenvolvimento.

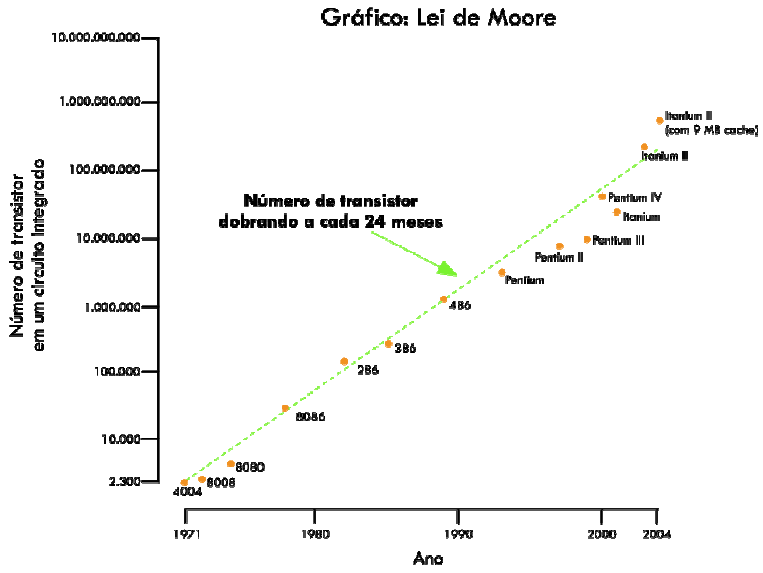

Figura 1: Gráfico da Lei de Moore. Figura retirada de harpiatec.com

Do ponto de vista físico, a Lei de Moore impõe um limite natural aos computadores, pois a partir do momento que fosse atingido o limite de um bit por átomo, não haveria mais como aumentar a densidade de bits por chip. Contudo, quando a escala atômica for atingida, o paradigma clássico da máquina de Turing deixa de ser válido, ou seja, devemos pensar num modelo de computação baseado nas leis da mecânica quântica. É justamente neste ponto que surge o que chamamos de Computação Quântica [12].

O *Q-BIT* E SUAS PROPRIEDADES

Infelizmente, o computador que estou utilizando para escrever este texto não é quântico. Nele, o processamento das informações ainda segue os paradigmas da física clássica. E ainda, em seu interior um *bit* pode ser simulado por um capacitor carregado ou não, pela magnetização de um disco rígido, ou ainda por qualquer outro mecanismo que nos forneça apenas um resultado de cada vez – ligado ou desligado

("0" ou "1"). Podemos fazer uma representação bastante simplória de um bit utilizando uma moeda. Para esse fim, representaremos o resultado 'cara' com o '0' e o resultado 'coroa' com o '1'. Conforme intuímos, a moedas são objetos macroscópicos, governados pela física clássica, e por isso só obtemos um dos resultados ("0" ou "1") em cada jogada. No entanto, se as moedas se comportassem como os objetos microscópicos, que obedecem os princípios da mecânica quântica, teríamos que as faces cara e coroa poderiam ser vistas ao mesmo tempo, ou seja, no lançamento de uma moeda, o resultado cara e coroa coexistiriam. Esse resultado é possível graças a uma das propriedades da mecânica quântica, denominada de superposição. Se novamente supusermos que uma moeda é um objeto quântico, os resultados '1' e '0' são denominados de estados e são representados por $|0\rangle$ e $|1\rangle$, e, nesse caminho, um *q-bit* (*bit* quântico) é representado por meio da expressão abaixo

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

onde α e β são números complexos, que fornecem a probabilidade de se encontrar $|0\rangle$ e $|1\rangle$, respectivamente, no lançamento de uma moeda. A superposição de estados, apesar de parecer um pouco estranha, pode ser entendida mediante uma analogia conhecida como gato de Schroedinger. Com o objetivo de explicar as minúcias das soluções da equação fundamental da mecânica quântica e do princípio da superposição, Schroedinger propôs o experimento imaginário no qual utiliza um gato que supostamente pode estar vivo ou morto ao mesmo tempo. Esse exemplo trata de uma forma simples de analisar o princípio da superposição das soluções da equação de Schroedinger [5, 6, 7, 8]. Tal princípio afirma que se para um determinado problema a equação de Schroedinger admitir duas soluções distintas $|a\rangle$ e $|b\rangle$, então o sistema pode ser descrito por meio da superposição das duas soluções, o que é matematicamente escrito como [2, 3]

$$|\varphi\rangle = |a\rangle + |b\rangle$$

onde os estados $|a\rangle$ e $|b\rangle$ existem simultaneamente. Contudo, quando observarmos o sistema, ou seja, quando efetuarmos uma medição, um dos estados colapsa (deixa de existir) e o outro é então detectado. Nesse sentido, o referido gato de Schroedinger faz alusão a essa curiosa propriedade quântica, conforme explicitamos a seguir. Considere um gato preso numa caixa onde há um recipiente com material radioativo que tem 50% de chance de emitir uma partícula radioativa a cada hora, e um contador Geiger. O contador Geiger é um aparelho utilizado para detectar radiação. Se o material liberar partículas radioativas, o contador percebe a sua presença e aciona um martelo, que, por sua vez, quebra um frasco de veneno. Evidentemente, ao se passar uma hora só terá ocorrido um dos dois casos possíveis: o átomo emitiu uma partícula radioativa ou não a emitiu (a probabilidade que ocorra um ou outro evento é a mesma). Como resultado da interação, no interior da caixa o gato estará vivo ou morto. Porém, isso não poderemos saber a menos que se abra a caixa para comprovar as hipóteses. Se tentarmos descrever o que ocorreu no interior da caixa, servindo-nos das leis da mecânica quântica, chegaremos a uma conclusão muito estranha. O gato viria descrito por uma função de onda extremamente complexa resultado da superposição de dois estados, combinando 50% de "gato vivo" e 50% de "gato morto". Ou seja, aplicando-se o formalismo quântico, o gato estaria por sua vez "vivo" e "morto"; correspondente a dois estados indistinguíveis! Assim, a função de onda que representaria o estado do gato seria dada por

$$|\varphi\rangle = |vivo\rangle + |morto\rangle.$$

A única forma de averiguar o que "realmente" aconteceu com o gato será realizar uma medida: abrir a caixa e olhar dentro. Em alguns casos encontraremos o gato vivo e em outros um gato morto. Isso ocorre por que ao realizar a medida, o observador interage com o sistema e o altera, rompendo a superposição dos dois estados, fazendo com o que o sistema seja observado em um dos dois estados possíveis. E isso é uma forma simplista de explicar o que chamamos de colapso da função de onda, que é uma característica inerente ao processo de medição em mecânica quântica. Nessa perspectiva, um *q-bit* pode existir num estado contínuo entre $|0\rangle$ e $|1\rangle$ até que ele seja observado. E então, quando um q-bit é medido, o resultado será sempre '0' ou '1', probabilisticamente. Vale destacar que os *q-bits* são objetos matemáticos com certas propriedades específicas que podem ser implementados como objetos físicos reais. Alguns exemplos de sistemas físicos que podem ser utilizados em computadores quânticos para representar *q-bits* são os seguintes: as polarizações diferentes de um fóton; o alinhamento de um spin nuclear em um campo magnético uniforme; os dois estados de um elétron orbitando ao redor de um átomo. Na seqüência do trabalho, detalharemos um desses sistemas como um exemplo.

Suponhamos agora que temos dois *qbits*. Se estivéssemos trabalhando com a computação clássica, teríamos quatro estados possíveis: 00, 01, 10 e 11. Como conseqüência, temos que um sistema de dois *qbits* possui quatro estados na base computacional: $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Contudo, de acordo com o princípio da superposição, exemplificado por Schroedinger mediante o seu famoso gato, um par de *qbit* também pode existir em superposições desses estados, ou seja, temos o seguinte estado

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle,$$

onde os coeficientes a, b, c e d são números complexos, sendo úteis nos cálculos de probabilidades. Na essência, um computador quântico manipula a informação, como se os quatro estados de dois *qbits* existissem ao mesmo tempo, e essa propriedade tornaria possível uma capacidade computacional muito além da que temos acesso na atualidade.

ALGORITMOS QUÂNTICOS

Qualquer pessoa que tenha algum conhecimento sobre computação, sabe que para um computador desenvolver determinada tarefa é necessário programá-lo. E, antes disso, é imprescindível elaborar um bom algoritmo. De uma forma simples, podemos dizer que um algoritmo é um conjunto de procedimentos necessários para se realizar uma determinada tarefa. Por exemplo, podemos elaborar uma algoritmo para trocar o pneu furado de um carro, onde percebemos que se duas etapas forem trocadas, o sucesso da tarefa estará comprometido (se o algoritmo não deixar claro que os parafusos devem ser afrouxados antes de se levantar o carro com o macaco). Nesse sentido, um programa será melhor na medida em que o algoritmo em que se baseia for mais eficaz. Felizmente, os nossos cientistas da computação, analistas de sistemas e outros profissionais correlatos são bastante competentes na elaboração de algoritmos para os computadores que temos hoje, de modo que existem inúmeros programas que facilitam as nossas vidas e permitem que leigos em computação, como eu, utilizem essa miraculosa máquina. Contudo, com o advento da computação quântica, esses programas ficarão obsoletos. Ou melhor, não somente esses programas, mas a teoria utilizada para elaborá-los ficará obsoleta. Dessa forma, quando essa nova revolução ocorrer, os programas deverão ser construídos a partir

de algoritmos quânticos. É justamente neste ponto que aparece um novo desafio, pois com esse novo paradigma, os futuros programadores deverão conhecer bem a forma como a informação deve ser tratada na perspectiva quântica, de forma que deter conhecimento sobre mecânica quântica deixará de ser um privilégio restrito aos físicos. Atualmente já existem alguns algoritmos quânticos propostos, que de certa forma apresentam considerável vantagem sobre os algoritmos clássicos. Um desses algoritmos quânticos foi desenvolvido por Peter Shor em 1993. Quando propôs o algoritmo, Shor trabalhava na empresa AT&T e desenvolvia pesquisas que apontavam vantagens dos computadores quânticos em relação à máquina de Turing. Nesse panorama, Shor formulou um algoritmo quântico que permitia decompor um número com muitos algarismos em seus fatores primos. O detalhe fundamental é que o algoritmo de Shor realiza essa tarefa em tempos muitos menores do que os gastos por algoritmos clássicos. O problema da fatoração é essencial para os sistemas criptográficos atuais, de forma que a proposição desse algoritmos põe em risco qualquer sistema de segurança (bancos, governos) a partir do momento em que o primeiro computador quântico começar a funcionar. Na Tabela 1 apresentamos algumas comparações entre o tempo de fatoração de números de tamanhos diferentes quando realizadas pelos computadores atuais e com o algoritmo de Shor. Observando a referida tabela percebemos o elevado potencial computacional dos sistemas quânticos. Notamos ainda que, os sistemas criptográficos de segurança baseados em chave pública ficarão totalmente obsoletos a partir do momento em que o primeiro computador quântico iniciar o seu funcionamento.

Tamanho do Número a Ser Fatorado (em bits)	Tempo de Fatoração por Algoritmo Clássico	Tempo de Fatoração por Algoritmo Quântico
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quadrilhões de anos	4,8 horas

Tabela 1: Comparação entre os tempos estimados para fatoração de números de tamanhos diferentes com o algoritmo clássico e com o de Shor. Fonte: Revista Ciência Hoje, Vol. 33, n. 193, Maio de 2003.

Um outro algoritmo quântico que merece destaque foi proposto pelo indiano Lev Grover em 1996, enquanto trabalhava nos laboratórios de pesquisa Bell, nos Estados Unidos. Grover propôs um algoritmo de busca, o qual, como o próprio nome já sugere, realiza a tarefa de buscar numa base de dados, encontrando itens que tenham certas propriedades desejadas. Estamos acostumados a utilizar algumas espécies de sistemas como esses quando usamos a internet. Assim como o algoritmo de Shor, a vantagem computacional apresentada pelo algoritmo de Grover chega a ser estupenda, pois em geral, numa determinada tarefa onde classicamente precisamos fazer n buscas, quanticamente são necessárias $\sqrt{n}$, que é um número muito menor. A título de ilustração, considere uma tarefa na qual classicamente necessitaríamos 10000 buscas; dessa maneira, quanticamente seriam necessárias apenas 100. O algoritmo de Grover pode ser aplicado com sucesso em problemas práticos da biologia molecular e engenharia genética. Assim, mediante esses dois exemplos de algoritmos quânticos, percebemos que computadores quânticos poderão, de fato, revolucionar a forma como tratamos a informação, sendo necessário para isso

que novos algoritmos quânticos sejam elaborados. Este é um grande desafio para o futuro da computação [12].

REDES NEURAIS E A COMPUTAÇÃO QUÂNTICA

Uma aplicação bastante interessante dos conceitos de computação quântica são as redes neurais. O modelo de redes neurais foi construído baseado no cérebro humano, pois este processa informações de uma maneira completamente diferente de um computador digital convencional. O cérebro pode ser considerado um computador altamente complexo, não- linear e paralelo, que por meio de seus constituintes chamados neurônios realiza processamentos, como percepção e controle motor, muito mais rapidamente do que qualquer moderno computador digital. Em seu livro Haykin [14] diz que o cérebro humano no momento do nascimento tem uma grande estrutura e a habilidade de desenvolver suas próprias regras através do que usualmente denominamos "experiência". Esta vai sendo acumulada com o tempo, sendo que o mais dramático desenvolvimento acontece durante os dois primeiros anos de vida e continua muito além desse estágio. Assim, um neurônio em "desenvolvimento" é sinônimo de um cérebro plástico em que a plasticidade permite que o sistema nervoso em desenvolvimento se adapte ao meio ambiente.

A plasticidade é fundamental para o funcionamento dos neurônios como unidades de processamento de informação do cérebro humano e também ela o é para a formação das redes neurais construídas com neurônios artificiais. Segundo Haykin uma rede neural, em sua forma mais geral, é uma máquina que é projetada para modelar a maneira como o cérebro realiza uma tarefa particular ou função de interesse; a rede é normalmente construída utilizando-se componentes eletrônicos ou é simulada por programação em um computador digital. Para esse autor, pode-se definir uma rede neural como uma máquina adaptativa da seguinte forma:

Uma rede neural é um processador maciçamente paralelamente distribuído, constituído de unidades de processamento simples, que têm a propensão natural para armazenar conhecimento experimental e torná-lo disponível para o uso. Ela se assemelha ao cérebro em dois aspectos:

O conhecimento é adquirido pela rede a partir de seu ambiente através de um processo de aprendizagem.

Forças de conexão entre neurônios, conhecidos como pesos sinápticos, são utilizados para armazenar o conhecimento adquirido.

O procedimento voltado ao processo de treinamento de aprendizado da rede é chamado de algoritmo de aprendizagem, cuja função é modificar os pesos sinápticos da rede de uma forma ordenada para alcançar um objetivo do projeto desejado. É possível também para uma rede neural modificar sua própria topologia, o que é motivado pelo fato dos neurônios do cérebro humano poderem morrer e que as novas conexões sinápticas possam crescer.

As redes neurais são também encontradas na literatura com os nomes de neurocomputadores, redes conexionistas, processadores paralelamente distribuídos, entre outros.

Benefícios de uma rede neural

Dois benefícios se destacam quando se fala em utilizar o método de redes neurais. O primeiro diz respeito a sua estrutura maciçamente paralela distribuída e o segundo é a sua habilidade de aprender e,

portanto, generalizar. A generalização se refere ao fato de a rede neural procurar saídas adequadas para entradas que não estavam presentes durante o treinamento (aprendizagem). Estas duas capacidades de processamento de informação possibilitam às redes neurais resolverem problemas complexos e muitas vezes intratáveis.

Embora o método de redes neurais possa resolver uma gama considerável de problemas, Andrade *et al* [15] deixam claro que existem limitações que impedem a resolução acurada de muitos desses problemas. Esses autores citam como exemplo o tempo de treinamento das redes neurais, que, dependendo do algoritmo de aprendizagem (Backpropagation, na maioria dos casos) tende a ser muito longo. Em alguns casos são necessários milhares de ciclos para se chegar a níveis de erros aceitáveis, principalmente se o algoritmo estiver sendo simulado em computadores que realizem operações de forma sequencial, já que o processador deve calcular as funções para cada unidade e suas conexões separadamente, o que pode ser problemático em redes muito grandes, ou com grande quantidade de dados.

A natureza multidisciplinar e as limitações de Redes Neurais Artificiais associadas à hipótese de que as sinapses – conexões – entre neurônios poderiam ser tratadas por fenômenos quânticos [16], motivaram o interesse de pesquisas em Redes Neurais que incorporassem conceitos de Física Quântica. Assim, o estudo de Redes Neurais Quânticas mostrou-se um ramo bastante inovador no campo da Computação Quântica embora seja uma área ainda incipiente [17, 18]. O trabalho realizado por Andrade *et al* [15] traz em seu bojo uma proposta de um modelo de neurônio quântico e descreve o seu funcionamento. O artigo também faz uma descrição dos princípios da computação quântica e Circuitos Quânticos. Segundo os autores o modelo proposto foi simulado utilizando o simulador de circuitos quânticos Zeno [19] desenvolvido na Universidade Federal de Campina Grande.

Herbster [20] no seu trabalho: O Estado da Arte em Redes Neurais Artificiais Quânticas relata que as Redes Neurais Quânticas surgiram como uma nova abordagem no campo da Computação Quântica, possuindo propriedades que permitem resolver os paradigmas encontrados nas Redes Neurais Clássicas. Na literatura é possível encontrar trabalhos [21–24] que evidenciam a importância da utilização de conceitos quânticos para mitigar ou até mesmo eliminar problemas inerentes aos métodos de computação clássica, uma vez que a computação Quântica tem como principais características o processamento e a transmissão de dados armazenados em estados quânticos de uma forma muito mais eficiente que os modelos de computação convencionais. Esses trabalhos fortalecem a ideia de que o advento da Física Quântica promoveu uma verdadeira revolução em todos os campos da tecnologia e em particular na computação.

TELEPORTE QUÂNTICO

Uma outra técnica da mecânica quântica que revela ser bastante aplicável na computação quântica é o teleporte quântico. Com o uso do teleporte quântico, podemos deslocar estados quânticos de um lugar para outro, mesmo quando não existe um canal de comunicação conectando o transmissor do estado ao seu receptor. De certa forma, podemos dizer que o teleporte é apoiado numa outra interessante propriedade da mecânica quântica denominada de emaranhamento. Para entender esta propriedade, considere uma superposição de estados constituída por duas componentes. O emaranhamento quântico

nos diz que se uma observação for feita sobre uma das componentes do sistema, essa observação afeta o resultado da observação feita sobre uma outra componente, que pode estar em um local bem distante da primeira, sem que haja qualquer interação entre elas [4]. Como um exemplo pictórico, tomemos dois irmãos, Paulo e João. Paulo mora no Brasil, enquanto João vive em Portugal. Suponha que Paulo e João tenham, cada um, camisetas de 4 cores distintas. Num dia qualquer, Paulo vai ao guarda-roupas e retira um das camisetas ao acaso. No mesmo momento, João também faz o mesmo. Se a propriedade do emaranhamento fosse aplicada a este caso, e as camisetas dos dois irmãos constituíssem estados emaranhados, quando observássemos a camiseta retirada por Paulo no Brasil, seria possível conhecer a cor da camiseta que João retirou em Portugal. E um detalhe interessante é que não houve qualquer comunicação entre os irmãos. O emaranhamento encontra diversas aplicações, dentre as quais se destacam as suas contribuições à computação quântica, informação quântica e teleporte quântico [4]. No entanto, apesar das incontáveis vantagens, o teleporte possui suas limitações, as quais discutiremos a seguir. A primeira limitação é que o teleporte quântico não nos permite transmitir informação mais rápido do que a luz. Na verdade, sem a comunicação clássica, o teleporte não transmite nenhuma informação. Esse fato pode ser compreendido a partir do exemplo citado anteriormente, pois alguém localizado em Portugal só saberá qual será a camisa que Paulo retirará em Portugal quando ficar sabendo qual foi a camisa que João retirou aqui no Brasil, ou seja, alguma outra pessoa aqui do Brasil deve, de maneira clássica, se comunicar com a referida pessoa de Portugal. Outra limitação do teleporte está relacionada com o fato deste procedimento não permitir a clonagem de um estado quântico. Com relação às vantagens apresentadas pelo teleporte quântico, podemos mencionar o seu uso na construção de portas lógicas resistentes aos ruídos e suas aplicações na técnica de códigos de correção de erros.

O TEOREMA DA NÃO-CLONAGEM

Uma outra propriedade da computação quântica que a difere bastante da computação clássica é referente ao teorema da não-clonagem. Este teorema, passível de demonstração, estabelece que é impossível copiar um estado quântico desconhecido [25, 26]. Classicamente, quando queremos copiar um bit clássico, aplicamos uma porta CNOT clássica, que toma o bit a ser copiado (em um estado *x* qualquer) e um bit em branco inicializado no estado 0. A saída do circuito é formada por dois bits no mesmo estado *x*. Sendo assim, como os dois bits aparecem iguais, clonamos o bit original. Do ponto de vista quântico, a porta CNOT quântica consiste basicamente em negar o segundo *q-bit* quando o primeiro for 1, e não alterar o segundo *q-bit* quando o primeiro for 0. Com o objetivo de exemplificar, suponha que se deseje copiar um *q-bit* em um estado desconhecido $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ da mesma forma que procedemos classicamente, ou seja, utilizando a porte CNOT. Nesse sentido, o estado dos dois *q-bits* na entrada pode ser escrito como:

$$[\alpha\,|0\rangle + \beta\,|1\rangle]\,|0\rangle = \alpha\,|00\rangle + \beta\,|10\rangle.$$

Após a aplicação da porta CNOT, o q-bit de saída será simplesmente $\alpha\,|00\rangle + \beta\,|11\rangle$. Percebemos que a cópia do circuito falhou, pois para um estado geral $|\varphi\rangle$, temos que:

$$|\varphi\rangle|\varphi\rangle = \alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \beta\alpha|01\rangle + \beta^2\,|11\rangle,$$

que é ligeiramente diferente de $\alpha\,|00\rangle + \beta\,|10\rangle$, pois em geral α e β são diferentes de zero. Percebemos assim, que de fato é impossível efetuar a cópia de um estado quântico qualquer. Essa é uma característica fundamental da computação quântica.

REALIZAÇÃO FÍSICA DE COMPUTADORES QUÂNTICOS

A computação quântica experimental está enfrentando atualmente um panorama muito parecido ao que a computação clássica encontrou na década de 30, pois não se sabia qual seria a melhor tecnologia para computadores [27, 28]. De forma análoga, diversas alternativas práticas estão sendo testadas para simular os *q-bits* da computação quântica, dentre as quais podemos citar: pontos quânticos, ressonância nuclear magnética em líquidos, armadilha de íons, supercondutores, dentre outros sistemas. Assim, vários protótipos de computadores quânticos, que utilizam pouco mais de uma dezena de *q-bits*, já foram testados com sucesso em laboratórios de todo o mundo. Esses testes demonstraram o funcionamento dos algoritmos quânticos descobertos até agora. O grande desafio atual é o aumento do número de *qbits* de forma controlada, e, certamente, as pesquisas pertinentes a esse tema se apoiarão na nanotecnologia. Nesse caminho, mesmo não sabendo qual seria a melhor tecnologia para o desenvolvimento dos computadores quânticos, já conhecemos os quatro requisitos básicos para a implementação experimental da computação quântica. Esses requisitos são os seguintes: (1) a representação dos *qbits*; (2) evolução unitária controlável; (3) preparação de estados iniciais de *qbits*; (4) medida do estado final dos *qbits*. No contexto desses requisitos básicos aparece uma dificuldade adicional na implementação dos computadores quânticos: ler os dados durante a execução do programa sem perder todo o processamento. Essa grande dificuldade emerge de um dos princípios da mecânica quântica que torna a computação quântica interessante, pois segundo a mecânica quântica, não é possível medir ou observar um sistema quântico sem destruir a superposição de estados. Porém, isso foi conseguido mediante a utilização de uma técnica conhecida como coerência de fase, a qual permite a correção de erros sem comprometer o sistema. Para esse fim, a técnica utiliza a observação indireta para efetuar a correção de erros e manter a coerência do sistema.

Nesse panorama de implementação física de computadores quânticos, merece destaque o trabalho realizado em dezembro de 2001 por um grupo de cientistas do Centro de Pesquisas da IBM, localizado em Almaden. Eles construíram um computador quântico de 7 *q-bits* e o utilizaram para fatorar o número 15. Apesar da simplicidade da experiência realizada, a máquina construída pôde comprovar a viabilidade da computação quântica, onde ficou evidente que as principais dificuldades encontradas até o momento são mais tecnológicas do que teóricas. O computador quântico da IBM foi implementado através de uma molécula com 7 *spins*, no sentido que o núcleo da molécula era constituído por 5 átomos de fluorina e 2 átomos de carbono. Do ponto de vista funcional, a programação do computador é realizada através de pulsos de rádio-frequência e a leitura dos dados é feita mediante o uso de técnicas de ressonância magnética nuclear (RMN). A operação desse computador quântico requer temperaturas baixas, a fim de reduzir a incidência de erros. Infelizmente, o computador quântico da IBM não está disponível para comercialização, por enquanto é apenas um instrumento de pesquisa. Mesmo assim, a aplicação desse tipo de máquina na solução de problemas criptográficos já despertou o interesse no departamento de defesa de diversos países.

CONCLUSÕES E PERSPECTIVAS

Realizamos neste trabalho uma revisão bibliográfica básica sobre a computação quântica, onde vimos que essa promissora área da ciência propõe a fusão entre as idéias da mecânica quântica e da ciência da computação. Notamos que apesar da incipiência de projetos para a construção de computadores quânticos, muitos desenvolvimentos mostraram-se possíveis e aplicáveis até mesmo na computação clássica. Percebemos também que a adoção do paradigma quântico na computação trata-se de um trajeto natural, pois caminha concomitante com a diminuição dos dispositivos eletrônicos presentes no computador, como já previa a Lei de Moore. Vale destacar que a computação quântica não é, como alguns podem erroneamente imaginar, mais uma dentre muitas tentativas de substituição de uma tecnologia em vias de esgotamento. Trata-se de um novo paradigma de computação, que pode ter profundas conseqüências, não só para a tecnologia, mas também para a teoria da informação, para a ciência da computação, e para a ciência em geral. Imaginamos que da mesma forma que a computação iniciada no século passado trouxe inúmeras aplicações que contribuíram para o desenvolvimento da humanidade nas mais variadas áreas, a computação quântica também propiciará aplicações que alcancem desde as viagens espaciais até a medicina, aumento assim a qualidade de vida das pessoas. Esperamos assim, que a forma pedagógica com que este artigo foi elaborado e a sua linguagem de fácil acesso possibilite que cada vez mais pessoas conheçam esse novo campo da ciência e, quem sabe, alguns não desenvolvam aptidão por pesquisar sobre esse vasto e frutífero tema.

AGRADECIMENTO

Agradecemos ao CNPq pelo suporte financeiro.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] PIRES, A. S. T. **Evolução das Ideias da Física**. São Paulo: Editora Livraria da Física, (2008).

[2] EISBERG, R.; RESNICK, R. **Física Quântica**. Rio de Janeiro: Editora Campus, (1979).

[3] COHEN-TANNOUDJI, C.; DIU, B.; LALOE, F. **Quantum Mechanics**. vol. 1, NY: Wiley Interscience, (1992).

[4] LANDAU, L. D.; LIFSHITZ, E. M. **Quantum Mechanics**. 3rd. Edition, Oxford: Pergamon Press, (1976).

[5] FEYNMAN, R. P., et al. **The Feynman Lectures on Physics**. Vol.3, NY: Addison-Wesley, (1982).

[6] PIZA, A. F. R. T. **Mecânica Quântica**. São Paulo: EDUSP, (2003).

[7] FREIRE, O. J.; PESSOA, O. J.; BROMBERG, J. L. **Teoria Quântica: estudos históricos e implicações culturais**. São Paulo: Livraria da Física, (2010).

[8] SAKURAI, J. J. **Modern Quantum Mechanics**: Revised Edition. NY: Addison-Wesley, (1994).

[9] GRIFFITHS, D. J. **Introduction to Quantum Mechanics**, Prentice Hall; (1995).

[10] SOUZA, A. M. C.**Tópicos de física contemporânea**. Sergipe, (2002).

[11] FAZZIO, A., et al. **Física para um Brasil competitivo**: Estudo encomendado pela Capes visando maior inclusão da Física na vida do país. Brasília: Sociedade Brasileira de Física, (2007).

[12] NIELSEN, M. A.; CHUANG, I. L. **Computação Quântica e Informação Quântica.** Porto Alegre: Bookman, (2005).

[13] GALVÃO, E., **O que é Computação Quântica?.**Rio de Janeiro: Vieira & Lent, 2007.

[14] Haykin, S., Neural Networks: A Comprehensive Foundation. 2a ed., New Jersey: Prentice Hall, 1999.

[15] Andrade, W. L., Araújo B. C., Gomes, H. M., Fechine, J. M. Proposta de um Neurônio Quântico. Congresso Brasileiro de Redes Neurais, 2005, Natal, RN, Anais do CBRN 2005, 2005 p. 1-5.

[16] Penrose, R. Shadows of the Mind. Vintage Science, 1994.

[17] Altaisky, M. V. Quantum neural network. Joint Institute for Nuclear Research, Russia. Technical report, Available online at the Quantum Physics repository: http://arxiv.org/PS_cache/quantph/pdf/0107012.pdf, las accessed 31/5/2004.

[18] Gupta, S., Zia, R. K. P. Quantum Neural Networks. Journal of Computer and System Sciences, vol. 63, pages 355 – 383, 2001.

[19] Cabral, G. E., Lula, B., Lima, A. F. Zeno: a New Graphical Tool for Design and Simulation of Quantum Circuits, Proceedings of SPIE Quantum Information and Computation III – Defense and Security Symposium, Orlando, 2005.

[20] Herbster, R. F., Andrade, W. L., Gomes, H. M., Machado, P. D. L. O Estado da Arte em Redes Neurais Artificiais Quânticas. Revista de Iniciação Científica da SBC, ano IV, Número IV, 2004.

[21] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5): 1484 – 1509, October, 1997.

[22] Deutsch, D. Quantum Computational Networks, Proceedings of the Royal Society of London, A 425, pages 73-90, 1989.

[23] Feynman, R. P. Simulating Physics with Computers, Int. J. Theor. Phys. Vol. 21, pages 467-488, 1982.

[24] Nielsen, M. A., Chuang, I. L. Quantum Computation and Quantum Information. Cambridge, UK, Cambridge University Press, 2000.

[25] RIEFFEL, E., WOLFGANG, P. **An Introduction to Quantum Computing for Non- Physicists.** ACM Computing Surveys, Vol. 32, No. 3, September 2000, pp. 300-335.

[26] GERSHENFELD, N., West, J. **The Quantum Computer.** Scientific American, 2000.

[27] SILVA, C.; MARTINS, R. **Revista Brasileira de Ensino de Física,** 18, n.4, (1996), 313.

[28] OLIVEIRA, I. S., et al, **Ciência Hoje**, vol. 33, n. 193, (2003), 22.