A LEI DE MOORE E OS AVANÇOS TECNOLÓGICOS: COMPUTAÇÃO QUÂNTICA

MAJ COM PAULO DE AQUINO LOPES FILHO

RESUMO: Paul Benioff, britânico criador da teoria de mecânica quântica aplicada à máquina de Turing, inventou a computação quântica em 1980. Em 1998, foi criado o primeiro compu-tador quântico experimental, iniciando a corrida para tornar a computação quântica uma realidade comercial. O interesse pela computação quântica visa a alcançar uma "vanta-gem quântica", ou seja, a capacidade de executar tarefas que não seriam possíveis em um computador clássico. Nas últimas décadas, houve um grande investimento público e privado na área em questão e, como consequência desse cenário, muitos avanços tecnológicos.

Palavras Chaves: COMPUTAÇÃO QUÂNTICA, TURING, VANTAGEM QUÂNTICA.

1. INTRODUÇÃO

O primeiro a prever a evolução do hardware foi Alan Turing em 1950, afir-mando que na virada do século teríamos computadores com memória na casa de 1 GB. Mais de uma década depois dessa afirmação, em um artigo de cunho científi-co na revista Eletronic Magazine de 19 de abril de 1965, Gordon Moore fez a se-guinte citação:

> "A complexidade para componentes com cus-tos mínimos tem aumen-tado em uma taxa de aproximadamente um fa-tor de dois por ano ... Certamente em um curto prazo pode-se esperar que esta taxa se mante-nha, se não aumentar. A longo prazo, a taxa de aumento é um pouco mais incerta, embora não haja razões para se acre-ditar que ela não se man-terá quase constante por pelo menos 10 anos. Is-so significa que em torno de 1975, o número de componentes por circuito integrado para um custo mínimo será 65 000 (65nM). Eu acredito que circuitos grandes como este poderão ser cons-truídos em um único componente (pastilha)."

Qualquer chip está ligado à lei de Moore, até mesmo o CCD de câmeras fotográficas digitais (sen-sores que captam a imagem nas câmeras de uso cotidiano) ou CNCL (sensores que captam ima-gens nas câmeras fotográficas pro-fissionais) (DISCO, 1998).

Em 1975, Moore revisou a sua previsão para, a cada dois anos, um aumento de 100% na quantidade de transistores dos chips mantendo seu custo. Porém um colega de Moore previu que esse período seria a cada 18 me-ses.

2. DESENVOLVIMENTO

2.1 A LEI DE MOORE

2.1.1 A LEI DE MOORE E A PRODUÇÃO

A lei de Moore tornou-se um objetivo para as indústrias de semicondutores, fazendo-as gastarem muitos recursos para poder alcançar as previsões de Moore no nível de desempenho e é isso que torna a Lei em questão realmente importante, pois sem ela, talvez não houvesse um desenvolvimento tão ace-lerado em nível de hardware e com cus-tos cada vez mais acessíveis.

2.1.2 CUSTO

A indústria de semicondutores teve de investir em Pesquisa & Desen-volvimento, fazendo com que houvesse a formulação de uma "segunda Lei de Moore" que previa um aumento no cus-to dos chips seguindo o aumento do desempenho. Isso ocorre pois a indús-tria de chips depende diretamente do custo de commodities como petróleo.

2.1.3 OS LIMITES DA LEI DE MOORE

Segundo a IBM, a aplicabilidade para a Lei de Moore pode estar chegando ao fim. Dentre os motivos está o fato de que os engenheiros estão desenvolvendo sistemas que exigem menos recursos do processador e os custos para pesquisas de novos processadores estão cada vez mais altos. Ainda, há o fato de que, com o aumento da velocidade, aumenta também o consumo de energia e a dissipação de calor.

No início de 2014, o departamento de pesquisa da IBM anunciou um teste de novos chips de silício com tecnologia de 7 nm empurrando para novos limites o pre-visto fim da Lei de Moore.

Em 2015, a IBM iniciou a caminha-da para a produção de processadores uti-lizando nanotubos de carbono, o que permitiria atingir escalas de 1,8 nm. Con-tudo, na tecnologia atual, fisicamente, o tamanho dos microchips é em torno de 5 nm.

Em outubro de 2019, a Google de-clarou ter alcançado a supremacia quân-tica, o que pode multiplicar consideravel-mente o poder de processamento.

2.2 A COMPUTAÇÃO QUÂNTICA

Um computador quântico é capaz de realizar cálculos utilizando-se das propri-edades da mecânica quântica, e isso já muda bastante o paradigma em relação à computação clássica.

Em comparação a um computador clássico, que funciona a partir da opera-ção de circuitos elétricos e portas lógicas manipulando bits, o computador quântico opera a partir de circuitos quânticos, ba-seados em portas lógicas quânticas, ma-nipulando a unidade fundamental, o q-bit (JORCUVICH, 2018).

2.2.1 ALGORITMOS E CIRCUITOS QUÂNTICOS

Para desenvolver determinada tare-fa a partir de um computador, é necessá-rio programá-lo e para isso é preciso de-senvolver um conjunto de procedimentos para executar essa tarefa, a esse conjunto de procedimentos dá-se o nome de “Algo-ritmo”.

Com a computação quântica, os programas deverão ser confeccionados a partir de algoritmos quânticos. Neste pon-to, aparece uma nova dificuldade, pois os futuros programadores deverão conhecer bem a forma como a informação deve ser tratada na perspectiva quântica. Os algo-ritmos quânticos nada mais são que apli-cações de circuitos quânticos. (JORCU-VICH, 2018).

2.2.2 PORTAS QUÂNTICAS

Similar à computação clássica, as portas lógicas quânticas realizam a fun-ção de um operador lógico atuando na informação, ou nos q-bits, e assim mani-pulando ou alterando o seu estado.

O conjunto de portas quânticas que realizam operações unitárias sobre um q-bit é infinito, pois as possibilidades de matrizes unitárias 2x2 também o são.

As matrizes unitárias garantem que a computação possa ser reversível (dado um q-bit j 1i em um estado arbitrário que passará pela porta quântica X, produzin-do o resultado j 2i e a porta quântica in-versa da X no q-bit j 2i, tem como resulta-do o q-bit inicial j 1i). Um vetor de estado (q-bit) deve ser unitário, e portanto, após a aplicação de uma porta quântica, haverá outro vetor de estado que continuará sendo unitário (JORCUVICH, 2018).

2.3 O HARDWARE

Segundo Jorcuvich, os primeiros protótipos de computador quântico apare-ceram em 1999, no MIT (Massachusettes Institute of Technology). Em 2007, a em-presa canadense **D−Wave** anunciou a construção do primeiro processador quân-tico do mundo, o Orion, com capacidade de processamento de 16 q-bits. Na se-quência, empresas como IBM e Google ampliaram esforços para o desenvolvi-mento de equipamentos similares.

Em 2017, a IBM anunciou ter fabrica-do um computador quântico de 50 q-bits. Em janeiro de 2018, foi a vez da Intel (49 q-bits) e em março, a Google (72 q-bits).

A capacidade computacional de um computador quântico é impressionante, por exemplo, um processador de 100 q-bits seria

mais poderoso do que a soma de todos os computadores atuais no pla-neta.

Nenhuma dessas empresas tentou inserir seus computadores quânticos no mercado. A perspectiva é que os compu-tadores quânticos entrem no mercado não para substituir completamente os PCs tradicionais, mas para integrá-los em um sistema mais poderoso.

Sua real eficácia foi comprovada re-centemente pela IBM, mostrando que computadores quânticos são muito mais rápidos do que os modelos tradicionais na resolução de alguns problemas

2.4 ALGORISMOS QUÂNTICOS

Os computadores quânticos são CONSTRUÍDOS para superar os compu-tadores clássicos, porém precisam execu-tar algoritmos quânticos. Os setores nos quais podem ser empregados incluem: criptografia, busca, otimização, simulação de sistemas quânticos e resolução de grandes sistemas de equações lineares. Alguns dos mais importantes, que além de demonstrarem a sua capacidade de cálculo, formam uma base para outros algoritmos, segundo Montanaro, em sua obra "Quantum Algorithms: an overview", de 2015:

> "• Deutsch-Jozsa é uma generalização do algo-ritmo de Deutsch. Este permite determinar se uma função é constante ou balanceada, mas des-ta vez a função possui múltiplos valores de en-trada;
> • Shor é fundamental pa-ra demonstrar o poder e a importância da compu-tação quântica.
> Este pode ser usado pa-ra fatorar números pri-mos, o que significa que ele pode ser
> usado para quebrar có-digos de criptografia, quando um computador quântico prático
> for construído. Este al-goritmo chamou a aten-ção de muitas pessoas;
> • Grover pode ser des-crito como um algoritmo de busca de banco de dados quântico.
> O algoritmo de Grover demonstra o poder de um computador quântico em que o algoritmo reduz significativamente o nú-mero de operações ne-cessárias para resolver o problema, em compara-ção com um computador clássico. Suas principais aplicações são na área de identificação de pa-drões, bioinformática, conectividade em grafos, encontrar o mínimo em uma lista não classifica-da de inteiros, etc;
> • Algoritmos de cami-nhada quântica que permitem projetar novos algoritmos quânticos mais eficientes e rápi-dos;
> • Algoritmos de simu-lação quântica que per-mitem simular compor-tamentos e propriedades quânticas como a equa-ção de schrödinger e te-letransporte;
> • Harrow resolve siste-mas de equações linea-res. O algoritmo estima o resultado de uma medida escalar no vetor solução para um dado sistema li-near de equações."

2.5 SIMULADORES DE CIRCUITOS QUÂNTICOS

As simulações desempenham um papel vital em diversas áreas de conheci-mento humano. Para a computação quân-tica, se tornou uma das alternativas mais viáveis para o estudo e o desenvolvimento da área.

O desenvolvimento de simuladores têm produzido ferramentas, tais como si-muladores de circuitos quânticos e lin-guagens de programação, os quais facili-tam a compreensão de algum aspecto relacionado à computação quântica.

Um simulador de circuitos quânticos permite descrever um algoritmo em ter-mos de portas e circuitos e testar esse al-goritmo para um estado quântico especí-fico através da simulação do hardware. A linguagem de circuitos quânticos descreve os principais algoritmos quânti-cos conhecidos. Ela é mais próxima dos físicos e dos engenheiros eletricistas, pois possui bastante similaridade com o seu análogo clássico que é amplamente conhecido.

Como a computação quântica é in-terdisciplinar, ou seja, envolve conheci-mentos de física, matemática e computa-ção, é salutar fornecer ferramentas que descrevam este

paradigma de forma inte-ressante para todas estas áreas.

Deve-se salientar que qualquer abordagem de simulação do paradig-ma computacional quântico em siste-mas clássicos sofrerá limitações. Ainda assim, a disponibilidade de um sistema computacional que permita uma descrição em nível apropriado de um algoritmo quântico e uma "máquina" para executar (ou simular) o algoritmo, facilitam tanto o ensino quanto o pró-prio desenvolvimento de algoritmos.

Nielsen sugere, que para projetar bons algoritmos, deve-se "desligar" da intuição clássica, parcialmente, e usar efeitos verdadeiramente quânticos.

2.5.1 EXEMPLOS DE SIMULADORES

Gustavo Cabral divide os Simu-ladores quânticos em dois tipos, os simbólicos e os universais. Os simbóli-cos são aqueles em que se desenvol-ve os algoritmos algebricamente. En-quanto os universais são aqueles que utilizam portas lógicas quânticas, em um circuito quântico.

Os simuladores escolhidos foram os universais pela usabilidade e didá-tica. Algoritmos quânticos são imple-mentados, principalmente, utilizando a ideia de circuitos. Além disso, outra divisão dos simuladores são os offline e online (JORCUVICH, 2018):

QCS – QUANTUM CIRCUIT SIMULATOR

É um aplicativo simples que permite simular o comportamento de portas quânticas básicas em celulares ou emuladores. Com ele é possível si-mular, em até seis q-bits, o compor-tamento de algumas portas . Após rodar a simulação, o aplicativo, for-nece as probabilidades de cada re-sultado. O aplicativo é intuitivo e utiliza um sistema de "arrastar e soltar" para a montagem dos circuitos.

O SIMULADOR ZENO

Foi desenvolvido em 2004, em Java, como trabalho de dissertação de mestrado de Gustavo Eulálio Ca-bral, pela Universidade de Campina Grande - PB. Apesar da última ver-são ser de 2006, é uma ferramenta didática completa. Um pouco mais completo que o QCS. Funciona em computadores pessoais. Conta com três tipos de saída: ket, matriz densi-dade e histograma.

IBM Q EXPERIENCE

É um processador quântico com 5 q-bits que pode ser acessado remotamente via internet através de uma plataforma de acesso manipulada pelo navegador, que permite manuseio tipo "arrastar e soltar" ou via linha de comando.

A plataforma permite simular o circuito nos servidores clássicos (disponibilizando até 20 q-bits), ou rodar no dispositivo real (computador quântico).

SIMULADOR QUIRK

Talvez o simulador universal mais completo disponível gratuita-mente. Desenvolvido por Craig Gid-ney.

O programa conta com diver-sos exemplos e recursos para cons-truir circuitos complexos e já dispo-nibiliza alguns circuitos em forma de portas lógicas. É possível também montar portas matricialmente e sal-vá-las para uso posterior no circuito.

3. CONCLUSÃO

O emprego da física quântica na computação parece ser uma ten-dência natural e ocorre em paralelo com a diminuição do tamanho dos dispositivos eletrônicos presentes nos computadores, como já previa a Lei de Moore.

O embasamento teórico ne-cessário tem início na matemática, em especial a álgebra e transita pela física moderna. O conhecimento dessas áreas é fundamental para o correto entendimento do assunto.

Os circuitos quânticos são a forma mais simples de compreender o funcionamento de computadores quânticos. A impossibilidade de construção de computadores quân-ticos em grandes escalas faz com que simulação deles em computado-res clássicos seja bastante empre-gada para desenvolver novos algo-

ritmos quânticos. É necessário tam-bém testá-los. Simuladores não devem apenas fornecer o resultado de cálculos, devem permitir a extração de informações sobre os algoritmos simulados. Posto isso, um bom simulador pode ser uma excelente ferramenta ao pesquisador.

4. REFERÊNCIAS

CASSINELLO, Andrés. O mistério quânti-co: uma expedição às fronteiras da física. São Paulo: Crítica, 2017. 270 p., [8] p. de estampas, il. (algumas col.), 24 cm. Inclui bibliografia. ISBN 9788542211436.

CROSS, Andrew W. , Lev S. Bishop, John A. Smolin e Jay M. Gambetta. Open quantum assembly language. ar-Xiv:1707.03429v2, 2017.

AMARAL, Bárbara, Alexandre T. Baraviera e Marcelo O. T. Cunha. Mecânica Quântica para Matemáticos em Formação. 28o Colóquio Brasileiro de Matemática - IMPA, 1o edição, 2011.

GIDNEY, Craig. Quirk quantum circuit simulator. http://algassert.com/2016/05/22/quirk.html. último acesso em 03/10/2022.

DEUTSCH, David. Quantum theory, the church-turing principle and the univer-sal quantum computer. Proceedings of the Royal Society of London, 1985.

DISCO, Cornelius; van der Meulen, Barend (1998). Getting new technologies to-gether (em inglês). New York: Walter de Gruyter. pp. 206–207. ISBN311015630X. OCLC39391108.

GALVÃO, Ernesto F. O que é Computação Quântica. Vieira e Lent, 1o edição, 2007.

CABRAL, Gustavo E. M. Uma ferramenta para projeto e simulação de circuitos quânticos. Dissertação de Mestrado, Centro de Ciênias e Tenologia da Univer-sidade Federal de Campina Grande, Bra-sil, 2004.

CARVALHO, Luiz M., Carlile C. Lavor e Vale-ria S. Motta. Caracterização matemática e visualização da esfera de bloch. TEMA Tend. Mat. Apl. Comput. SBMac, 2007.

FAYNMAN, Richard P. Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7), 1982.

BRAVYI, Sergey. David Gosset e Robert König. Quantum advantage with shal-low circuits. Science, 2018.

DRAPER, Thomas G. Addition on a quan-tum computer. arXiv:quant-ph/0008033, 2000.