Universidade de São Paulo
Instituto de Matemática e Estatistica
IME

Computação Quântica

Patrícia da Silva Rodrigues (nºUSP 11315590),
Samantha Miyahira (nºUSP 11797261),
Sabrina Araújo da Silva (nºUSP 12566182),

Dezembro
2022

Sumário

Parte I
O que é Computação Quântica?

A computação quântica é um tipo de computação que usa os princípios da física quântica para resolver problemas matemáticos. A mecânica quântica apresenta fenômenos que são usados como inspiração para o tratamento de dados de uma forma que os computadores atuais são incapazes de fazer.

Os computadores quânticos usam os chamados *qubits* (bits quânticos para a manipulação e armazenamento de dados). A grande diferença entre os bits clássicos e os bits quânticos é que, diferentemente do que ocorre com os bits clássicos, que ou são 0 ou são 1, os bits quânticos podem representar 0, 1 e 0 e 1 simultaneamente. Esse tipo de representação pode aumetar e muito a velocidade dos cálculos em comparação aos computadores que operam apenas em binário.

Problemas como a fatoração de grandes números e otimização de sistemas complexos são considerados grandes problemas da computação convencional e os computadores quânticos têm o potencial de resolver esses tipos de problemas. Esse tipo de otimização é de grande relevância para o futuro e avanço da técnologia computacional. Apesar de todo potencial tecnológico dos computadores quânticos, a implementação do hardware ainda é um desafio para a área.

Parte II
História

A origem da computação quântica pode ser traçada desde o início do século 20, com o desenvolvimento da mecânica quântica por físicos como Erwin Schrödinger, Niels Bohr e Werner Heisenberg, que quebraram diversos paradigmas da física quântica. Entre eles, podemos citar:

- Superposição Quântica;
- Gato de Schrödinger;

- Entrelaçamento Quântico;
- Teletransporte Quântico;
- Espalhamento de Rutherford;
- Existência de multiverso.

Na década de 50, já pensavam sobre como seria a aplicação das leis da física e da mecânica quântica nos computadores. No entanto, apenas em 1982 que o físico Richard Feynman introduziu **a concepção da máquina quântica de Turing**, que se trata de um modelo teórico de um computador quântico baseado nos princípios da mecânica quântica.

A busca de Richard Feynman sobre os computadores quânticos inspirou muitos outros pesquisadores da área a explorar o potencial da computação quântica e dos computadores quânticos. Atualmente, as contribuições teóricas de Richard Feryman são de grande relevância acadêmica e o modelo das máquinas quânticas de Turing são exploradas na área de computação quântica.

Outro pioneiro na história da computação quântica foi David Deutsch, da Universidade de Oxford, que, em 1985, descreveu o primeiro computador quântico, conhecido como máquina de Turing.

Depois desse período de desenvolvimento da computação quântica, em 1994, o professor de matemática Peter Shor, da Bell Labs, desenvolveu o **Algoritmo de Shor** para computadores quânticos capaz de fatorar grandes números numa velocidade muito superior a algoritmos de computadores convencionais. Em particular, o algoritmo é potencialmente capaz de quebrar certos algoritmos criptograficos que são considerados seguros até então para a proteção de dados e comunicação. O Algoritmo de Shor, portanto, foi um dos maiores demonstrativos da capacidade de computadores quânticos até então.

Em 1996, Lov Grover, também da Bell Labs, desenvolveu o primeiro algoritmo de busca em bases de dados quânticas, chamado **Algoritmo de Grover**, que tem aplicações potenciais para uma ampla gama de campos da ciência.

Na mesma época, foi apresentado o primeiro modelo de correção de erros quânticos gerados por computadores quânticos, isso porque há uma aproximação para que esses computadores sejam capazes de processar grandes números de qubits por longos períodos de tempo.

Esses erros poderiam então ser sobrescritos e isso pode vir a ser o segredo para que computadores quânticos possam ir para a produção em grande escala. No entanto, as propostas possuiam algumas limitações, o que faz com que a área de pesquisa sobre esses erros continua ativa até os dias atuais.

Apesar de todo o arcabouço teórico desenvolvido até o momento, foi apenas em 1999 que, no MIT, foram desenvolvidos os primeiros computadores quânticos.

Em 2014, a empresa Canadense D-Wave afirmou ter desenvolvido um computador híbrido chamado Orion que inclui um processador quântico de 16 qubits, mas que também processa bits convencionais. [6]

Em 2017, A D-Wave Systems lançou comercialmente o 2000Q, um computador quântico de 2000 qubits a módicos US 15 milhões. O computador quântico anterior da companhia tinha 1.000 qubits. Os sistemas de 1.000 quibits da empresa canadense estão sendo testados pelo Google, NASA e pela Lockheed Martin. [12]

Ainda em 2017, o brasileiro Guilherme Tosi, juntamente com pesquisadores da Universidade de Nova Gales, na Austrália, inventou uma nova arquitetura para a computação quântica, baseada em flip-flops qubits, que pode ser usada como um novo tipo de computador quântico, algo que poderia permitir a fabricação de processadores quânticos em larga escala de uma maneira muito mais barata e fácil do que se imaginou ser possível.

No ano de 2019, um artigo científico publicado pela NASA afirma que a Google criou um computador quântico chamado Sycamore para realizar uma série de operações em 200 segundos que levariam um supercomputador cerca de 10.000 anos para realizar. [7]

Em 2022, a empresa instalou o primeiro computador quântico na universidade do sul da Califórnia, chamada de sistema Advantage. [6]

Parte III

Princípios da Computação Quântica

Na computação quântica, a unidade de informação básica é o Bit quântico ou q-bit. Como foi dito na Parte I, um bit-quântico é uma unidade de informação quântica, é análogo ao bit clássico, que é uma unidade binária de armazenamento de informação nos computadores clássicos. Em computadores quânticos, um qubit pode ser 0, 1 e 0 e 1 ao mesmo tempo, graças ao fenômeno de superposição quântica, algo que remete a experiência mental do **Gato de Schrödinger**, no qual a experiência de superposição é emulada. Isso signfica que um qubit pode armazenar mais de uma unidade de informação, algo que permite que computadores quânticos possam realizar cálculos muito mais rapidamente que computadores convencionais.

Os q-bits são representados por vetores de estados em um sistema quântico de dois níveis, o que equivale a um vetor em um espaço bidimensional sobre números complexos:

Essa é a representação matemática do q-bit

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

Os estados do q-bit podem ser representados da seguinte forma:

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

O conjunto $\{|0\rangle, |1\rangle\}$ forma uma base de Hilbert de duas dimensões, conhecida como base computacional.

Base de Hilbert ou base Hilbertiana [8]:

Seja H um espaço de Hilbert.

Um subconjunto $\mathrm{B} = (x_i)_{i\in I}\mathrm{B} = (x_i)_{i\in I} deH$ **H** é dito uma **base Hilbertiana** de **H** se:

B é um conjunto ortonormal, isto é,

$$\langle x_i, x_j\rangle = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases},$$

para todos $x_i, x_j \in \mathrm{B} x_i, x_j \in \mathrm{B}$; o conjunto gerador por B
B for denso em H, ie, $\overline{\operatorname{span} \mathrm{B}} = H$

Para a manipulação dos estados quânticos, utiliza-se principalmente radiação eletromagnética. A radiação eletromagnética é um tipo de energia transmitida pelo espaço como uma onda. As portas lógicas quânticas são blocos básicos de construção de computadores quânticos.

As portas lógicas quânticas podem ser usadas para fazer operações lógicas básicas, como AND, OR e NOT, mas também operações complexas, como a **Transformada de Fourier Quântica (QFT)** e correção quântica de erros.[9]

Exemplo: Transformada de Fourier Quantica[9][10][11]

Definição:

A transformada de Fourier quântica é a transformada de Fourier discreta clássica aplicada ao vetor de amplitudes de um estado quântico, onde geralmente consideramos vetores de comprimento $N = 2^n$

A transformada de Fourier clássica utiliza um vetor do tipo

$x = (x_0, x_1, \ldots, x_{N-1}) \in C^N$

(espaço n-ésimal complexo) e mapeia para o vetor

$y = (y_0, y_1, \ldots, y_{N-1}) \in C^N$ através da seguinte fórmula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{-kn}, \quad k = 0, 1, 2, \ldots, N-1,$$

Onde,

$\omega_N = e^{\frac{2\pi i}{N}} \omega_N = e^{\frac{2\pi i}{N}} e \omega_N^n \omega_N^n$ é um N^{th} raiz da unidade .

Da mesma forma, a transformada quântica de Fourier atua em um estado quântico
$|x\rangle = \sum_{i=0}^{N-1} x_i |i\rangle$ e mapeia para um estado quântico $\sum_{i=0}^{N-1} y_i |i\rangle$ de acordo com a fórmula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{nk}, \quad k = 0, 1, 2, \ldots, N-1,$$

Observe que a alteração no sinal do expoente fazem com que o fator de fase varie. Na aplicação acima, a transformada quântica de Fourier age como a transformada de Fourier discreta e vice-versa.

Em caso de $|x\rangle$ é um estado básico, a transformada quântica de Fourier também pode ser expressa como o mapa

$$\text{QFT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{xk} |k\rangle.$$

Por fim, podemos mostrar que a transformada quântica de Fourier pode ser vista como uma matriz unitária com portas lógicas quânticas (parecida com portas lógicas booleanas em computadores convencionais) que agem sobre os vetores de estado quântico.

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

Onde $\omega = \omega_N$.

Obtemos, por exemplo, no caso de $N = 4 = 2^2 fase \omega = i$ a matriz de transformação

$$F_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} F_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

(OBS: Os cálculos acima que demonstram como seria uma Transformada Quântica de Fourier em comparação com a Transformada clássica de Fourier foram retirados da literatura referênciada no título e estão em [9][10] e [11])

A transformada de Fourier quântica, inventada por Don Coppersmith, é utilizada em algoritmos quânticos, como é o caso do **Algoritmo de Shor** para fatorar e calcular o logarítmo discreto, entre outros cálculos. [9]

A transformada quântica de Fourier, utilizada em um computador quântico, pode realizar de forma eficiente a decomposição par-

ticular em um produto de matrizes unitárias mais simples. Usando a decomposição simples, a transformada de Fourier de complexidade $O(2^n)$ pode ser implementada como um circuito quântico, consistindo em apenas $O(n^2)$ portões Hadamard e portões de mudança de fase controlada, no qual n é o número de qubits. [10]

A Transformada Quântica de Fourier trabalha em um estado quântico, enquanto a Transformada clássica de Fourier trabalha com vetor. Portanto, nenhuma execução que usa a Transformada clássica de Fourier é capaz de executar uma função mais optimizadamente que compense essa aceleração exponencial, enquanto as execuções que utilizam a transformada quântica de Fourier exigem apenas **O(n log n** portas lógicas.

Parte IV

Problemas Computacionais Complexos e a Computação Quântica

Otimização de problemas matemáticos computacionais:

Os problemas de otimização envolvem encontrar a melhor solução possível entre um conjunto de problemas viáveis, dadas algumas restrições e regras que envolvem o problema em questão. Esses problemas podem ser resolvidos através de diferentes técnicas matemáticas, como programação linear e não linear, programação dinâmica, etc. Os computadores quânticos, por outro lado, utilizam fenômenos da mecânica quântica, como emaranhamento[8] e superposição, para a operação com dados de problemas matemáticos complexos.

Os computadores quânticos têm maior potencial de solucionar problemas matemáticos complexos do que os computadores estritamente binários convencionais, devido a sua capacidade de pesquisar um grande número de soluções possíveis pertencentes a um conjunto de soluções viáveis de maneira simultânea.

Um exemplo interessante é o **Problema do Caixeiro Viajante**, pertencente a classe NP-Difícil. Trata-se de um problema de fatoração de grandes números. Suponha que um caixeiro via-

jante tenha de visitar n cidades diferentes, iniciando e encerrando sua viagem na primeira cidade. Suponha, também, que não importa a ordem com que as cidades são visitadas e que de cada uma delas pode-se ir diretamente a qualquer outra. O problema do caixeiro viajante consiste em descobrir a rota que torna mínima a viagem total [1]. A solução para esse problema está em $(n-1)! = (n-1).(n-2).(n-3).(n-4).....2.1$. A velocidade com que o fatorial cresce faz com que o aumento do tempo de processamento aumente também muito rapidamente, como na figura abaixo.

n	rotas por segundo	(n - 1)!	cálculo total
5	250 milhoes	24	insignific
10	110 milhoes	362 880	0.003 seg
15	71 milhoes	87 bilhoes	20 min
20	53 milhoes	1.2×10^{17}	73 anos
25	42 milhoes	6.2×10^{23}	470 milhoes de anos

A solução quântica encontrada para o problema supracitado é através da técnica Simulated Annealing (Recozimento simulado) [2]. O recozimento simulado é uma meta-heurística de busca local estatística usada para resolver problemas de otimização discretos e, em menor grau, contínuos. A principal característica do recozimento simulado é que ele fornece um meio de escapar dos ótimos locais, permitindo movimentos de subida (ou seja, movimentos que pioram o valor da função objetivo) na esperança de encontrar um ótimo global. [2]

Problemas de aprendizado de máquina:

São problemas que envolvem o uso de dados para treinar um modelo para fazer previsões e decisões. Os exemplos incluem reconhecimento de imagem, processamento de linguagem natural e modelagem preditiva.

O primeiro kit de ferramentas e biblioteca de **Processamento Quântico de Linguagem Natural** foi anunciado pela Cambridge

Quantum("CQ") em 15 de Outubro de 2021. O lambeq é o primeiro kit de ferramentas de software para QNLP do mundo capaz de converter frases em um circuito quântico. Ele foi projetado para acelerar o desenvolvimento de aplicações práticas de QNLP do mundo real, como diálogo automatizado, mineração de textos, tradução de idiomas, conversão de texto em fala, geração de linguagem e bioinformática. [3]

Problemas de Criptografia de Dados:

São problemas que envolvem o uso de algoritmos matemáticos para criptografar e descriptografar dados. Exemplos incluem segurança de dados, privacidade online e comunicação segura.

Criptografia é a prática de comunicação segura na presença de terceiros, geralmente envolvendo o uso de algoritmos matemáticos para codificar e decodificar mensagens.

A criptografia classica pode vir a ser ameaçada e a solução para isso está junção da computação quântica com a criptografia para o desenvolvimento de algoritmos criptográficos resistentes a quantum. Os algoritmos criptográficos clássicos geralmente são projetados para serem computacionalmente impossíveis de quebrar, mas essa segurança pode ser comprometida caso a invasão ocorra por meio de um computador quântico. Os computadores quânticos, por terem recursos quânticos que os tornam muito mais rápidos que os computadores convencionais, podem executar certas operações muito mais rapidamente, potencialmente permitindo que alguns algoritmos criptograficos, atualmente considerados seguros, sejam quebrados. Para o problema, alguns pesquisadores estão projetando novos algoritmos criptograficos especificamente para serem resistêntes a ataques de computadores quânticos.

O algoritmo mais comumente associado com a criptografia é o one-time pad, pois ele tem comprovadamente uma segurança perfeita [1] quando usado com uma chave aleatória e do mesmo tamanho que a mensagem. [4]

O **One-Time Pad** (OTP) é uma técnica quântica considerada teoricamente inquebrável, desde que utilizada corretamente. A técnica consiste no uso de uma chave gerada aleatóriamente com o mesmo comprimento da mensagem que está sendo criptografada. A chave é usada para XOR da mensagem, resultando em uma mensagem criptografada que parece completamente aleatória. Para des-

criptografar a mensagem, o destinatário usa a mesma chave para XOR da mensagem criptografada. Não existem propriedades estatísticas que possam ser exploradas para quebrar a criptografia. Como resultado, o One-Time Pad e considerado forma mais segura de criptografia, desde que a chave seja um segredo.A ideia da chave de uso único deriva da crifra de Vernam, em homenagem a Gilbert Vernam, um de seus inventores. O uso único da chave veio apenas posteriormente, quando Hoseph Maugorgne percebeu que se a fita fosse totalmente aleatória, a criptoanálise poderia ser impossível. [5]

No caso do OTP, não é impossível que um computador quântico seja capaz de quebrar a criptografia usando um algoritmo quântico para pesquisar um grande número de chaves possíveis mais rapidamente que um computador convencional. No entanto, isso exigiria que o computador quântico fosse suficientemente mais poderoso que qualquer computador existente nos dias atuais. No entanto, considerando que isso é uma possibilidade, pesquisadores estão debatendo sobre essa questão à medida que a computação quântica, ainda recente, se desenvolve.

A partir das análises, é importante ressaltar que os computadores quânticos ainda são muito recentes e que não há uma dimensão completa sobre o potencial quantico na computação e na área de segurança de dados. Portanto, o uso de algoritmos clássicos de segurança de dados como o OTP ainda continuarão sendo extremamente relevantes na segurança de dados.

Parte V
Expectativas para o Futuro

Podemos concluir que a computação quântica faz parte de um processo natural de evolução da tecnologia de computação e que um grande diferencial da computação quântica, que trás essa quebra de paradigma, é que os limites físicos e lógicos dos componentes presentes em computadores convencionais, que são super eficientes na execução de diversas tarefas, mas não para outras muitas, podem ser superados com a tecnologia quântica. Muitas tarefas executadas hoje por computadores convensionais, que envolvem tecnologias realmente relevantes, como a inteligência artificial, criptografia, pro-

blemas de otimização, entre outros, apesar de serem executadas, exigem um processamento muito intenso que, para alguns problemas complexos, podem exigir milhares de anos de processamento, algo que é na prática inviável. Portanto, a computação quântica coloca à vista da ciência um horizonte cheio de expectativas e que ainda precisa ser desbravado.

Podemos dizer que a expectativas para o desenvolvimento de algumas áreas da ciências através da tecnologia quântica, apesar de se tratar de algo ainda difícil de predizer, são grandes. Áreas como:

- Descobertas no campo farmacêutico: Computadores quânticos têm potencial de simular complexas reações químicas, algo que pode acelerar o descobrimento de novas drogas;
- Inteligência Artificial: Computadores quântios têm o potencial de otimizar o aprendizado de máquina;
- Otimização: Computadores quânticos podem resolver de maneira muito mais eficiente diversos problemas atuais que não possuem solução rápida;
- Criptografia: Computadores quânticos têm o potencial de quebrar algoritmos criptograficos que hoje são considerados seguros;

Por fim, espera-se que a computação quântica esteja em diversos setores e campos de pesquisa nos próximos anos, a medida que a tecnologia continue a evoluir e se torne mais amplamente disponível.

Parte VI

Referências

[1]: Problema do Caxeiro Viajante

[2]: A Teoria e Prática do Recozimento Simulado

[3]: Primeiro kit de ferramentas e biblioteca de processamento quântico de linguagem natural do mundo

[4]: C.E. Shannon, A Mathematical Theory of Communication, Bell System Technical Journal, July (1948) p.379; October (1948) p.623.

[5]: Kahn, David (1996). The Codebreakers. [S.l.]: Macmillan. pp. 397–8. ISBN 0-684-83130-9

[6]: SIte: dwavesys

[7]: Google claims it has finally reached quantum supremacy. Newscientist

[8]: Emaranhamento quântico finalmente é provado. HypeScience.

[9]: Coppersmith, D. (1994). «An approximate Fourier transform useful in quantum factoring.». Technical Report RC19642, IBM

[10]: Michael Nielsen and Isaac Chuang (2000). Quantum Computation and Quantum Information. Cambridge University Press. Cambridge: [s.n.] ISBN 0-521-63503-9. OCLC 174527496

[11]: Hales, L.; Hallgren, S. (November 12-14, 2000). «An improved quantum Fourier transform algorithm and applications». Proceedings 41st Annual Symposium on Foundations of Computer Science: 515–525.

[12]: Artigo: Silicon quantum processor with robust long-distance qubit couplings Autores: Guilherme Tosi, Fahd A. Mohiyaddin, Vivien Schmitt, Stefanie Tenberg, Rajib Rahman, Gerhard Klimeck, Andrea Morello Revista: Nature Communications Vol.: 8, Article number: 450