Computação Quântica

Ísis Ardisson Logullo

8 de Janeiro de 2022

1 Introdução

A Computação Quântica é uma subárea da Ciência da Computação que desenvolve tanto a tecnologia computacional baseada nos princípios da teoria quântica quanto o software que é executado no computador quântico. Estuda aplicações das teorias e propriedades da mecânica quântica, seu principal foco é o desenvolvimento do computador quântico. Seguindo as leis da mecânica quântica, este ganha grande poder de processamento pela capacidade de estar em vários estados e de realizar tarefas simultâneas.

Na computação clássica o computador é baseado na arquitetura de Von Neumann, que possui processador e memória destacados por um barramento de comunicação, sendo seu processamento sequencial. A Lei de Moore afirma que a velocidade de um computador é dobrada a cada 12 meses. Assim sempre houve um crescimento constante na velocidade de processamento dos computadores. Mas essa evolução tem um certo limite. Assim a necessidade do desenvolvimento de uma máquina extremamente eficiente se torna maior a cada dia.

Os computadores quânticos são uma nova era de máquinas que têm potencial de usar a IA para resolver problemas que levariam muito tempo com os computadores convencionais. Essas máquinas quânticas processam informações de maneiras e dimensões totalmente diferentes dos computadores usados atualmente em sistemas de IA. Enquanto os computadores convencionais processam informações como uma série de 0s e 1s (código binário), as máquinas quânticas podem usar esses 0s e 1s simultaneamente. A capacidade que eles têm de realizar muitos cálculos ao mesmo tempo reduz significativamente o tempo de processamento. Com os computadores quânticos, os sistemas de IA podem concluir em segundos tarefas que levariam milhares de anos nos supercomputadores mais rápidos. Desse modo, os pesquisadores podem encontrar respostas para problemas complexos quase instantaneamente.

2 História

- 1959 — Richard Feynman afirma a possibilidade de usar efeitos quânticos para computação.
- 1968 — Stephen Wiesner inventa a codificação conjugada que é uma ferramenta criptográfica. É parte dos dois aplicativos que Wiesner descreveu para codificação quântica, junto com um método chamado de multiplexação quântica, usa fótons polarizados em bases conjugadas como *q-bits* para passar informações. A codificação conjugada também é uma extensão simples de um gerador de números aleatórios. O conceito inicial de criptografia quântica desenvolvido por Bennett e Gilles Brassard também foi baseado neste conceito.
- 1970 — James Park articula o teorema da não clonagem.
- 1973 — Alexander Holevo publica um artigo mostrando que n q-bits podem transportar mais de n bits clássicos de informação, mas no máximo n bits clássicos são acessíveis (um resultado conhecido como *teorema de Holevo* ou *limite de Holevo*). Charles H. Bennett mostra que o cálculo pode ser feito de forma reversível.
- 1975 — R. P. Poplavskii publica *Modelos termodinâmicos de processamento de informação* que mostrou a inviabilidade computacional de simular sistemas quânticos em computadores clássicos, devido ao princípio de superposição.
- 1976 — O físico matemático polonês Roman Stanislaw Ingarden publica *Quantum Information Theory*. É uma das primeiras tentativas de criar uma teoria da informação quântica, mostrando que a teoria da informação de Shannon não pode ser diretamente generalizada para o caso quântico, mas sim que é possível construir uma teoria quântica da informação dentro do formalismo de uma mecânica quântica generalizada de sistemas abertos e um conceito generalizado de observáveis.
- 1980 — Paul Benioff descreve o primeiro modelo de mecânica quântica de um computador. Neste trabalho, Benioff mostrou que um computador pode operar sob as leis da mecânica quântica, descrevendo uma descrição da equação de Schrödinger das máquinas de Turing, estabelecendo uma base para trabalhos futuros em computação quântica. Yuri Manin brevemente motiva a ideia da computação quântica. Tommaso Toffoli apresenta a porta de Toffoli reversível, junto com as portas NOT e XOR, fornece um conjunto universal para computação clássica reversível.

- 1981 — Primeira Conferência sobre Física da Computação Paul Benioff e Richard Feynman dão palestras sobre computação quântica. Benioff baseado no seu trabalho do início de 1980, mostrou que um computador pode operar sob as leis da mecânica quântica. Feynman observou que parecia impossível simular com eficiência uma evolução de um sistema quântico em um computador clássico e propôs um modelo básico para um computador quântico, incitando o mundo a construí-lo.

- 1982 — Proposta de computador quântico por Paul Benioff baseado no trabalho de Charles Bennett de 1973, desenvolvendo ainda mais seu modelo original de máquina de Turing mecânica quântica. William Wootters e Wojciech Zurek, e independentemente Dennis Dieks redescobrem o teorema da não clonagem.

- 1984 — Charles Bennett e Gilles Brassard descobrem o protocolo de criptografia quântica BB84.

- 1985 — David Deutsch cria o primeiro algoritmo quântico. Ele descreve o primeiro computador quântico universal. Assim como uma máquina de Turing universal pode simular qualquer outra máquina de Turing com eficiência (tese de Church-Turing), o computador quântico universal é capaz de simular qualquer outro computador quântico com, no máximo, uma desaceleração polinomial. Asher Peres aponta a necessidade de esquemas de correção de erros quânticos e discute um código de repetição para erros de amplitude.

- 1988 — Yoshihisa Yamamoto e K. Igeta propõem a primeira realização física de um computador quântico, incluindo a porta CNOT de Feynman. A abordagem usa átomos e fótons e é o progenitor da computação quântica moderna e dos protocolos de rede usando fótons para transmitir q-bits e átomos para realizar operações de dois q-bit.

- 1989 — Gerard J. Milburn propõe uma realização ótica quântica de uma porta de Fredkin. Bikas K. Chakrabarti propõe a ideia de que as flutuações quânticas podem ajudar a explorar paisagens energéticas acidentadas, sugerindo a eficácia do recozimento quântico sobre o recozimento simulado clássico.

- 1992 — David Deutsch e Richard Jozsa propõem um problema computacional que pode ser resolvido eficientemente com o algoritmo determinista de Deutsch-Jozsa em um computador quântico, mas para o qual nenhum algoritmo clássico determinístico é possível. Este foi talvez o primeiro resultado na complexidade computacional dos computadores quânticos,

provando que eles eram capazes de realizar algumas tarefas computacionais bem definidas com mais eficiência do que qualquer computador clássico.

- 1993 — Descoberto o teleporte quântico por Charles Bennett e colaboradores.
- 1994 — Peter Shor descobriu um algoritmo quântico, que permite a um computador quântico fatorar grandes inteiros exponencialmente com muito mais rapidez do que o algoritmo clássico mais conhecido. O algoritmo de Shor pode teoricamente quebrar muitos dos sistemas de criptografia de chave pública em uso hoje.
- 2000 — Arun K. Pati e Samuel L. Braunstein provaram o teorema quântico de não exclusão. Isso é dual para o teorema da não clonagem, que mostra que não se pode deletar uma cópia de um q-bit desconhecido. Juntamente com o teorema de não clonagem mais forte, o teorema de não exclusão tem implicações importantes, ou seja, a informação quântica não pode ser criada nem destruída. Primeiro computador de RMN de 5 e de 7 q-bit em funcionamento demonstrado.
- 2001 — É demonstrado o algoritmo de Shor por RMN. Noah Linden e Sandu Popescu provaram que a presença de emaranhamento é uma condição necessária para uma grande classe de protocolos quânticos. Isso, juntamente com o resultado de Braunstein, colocou em questão a validade da computação quântica de NMR. Emanuel Knill, Raymond Laflamme e Gerard Milburn mostram que a computação quântica óptica é possível com fontes de fóton único, elementos ópticos lineares e detectores de fóton único, lançando o campo da computação quântica óptica linear.
- 2004 — Primeiro computador quântico de NMR de estado puro (baseado em para-hidrogênio) demonstrado. Primeiro emaranhamento de cinco fótons demonstrado pelo grupo de Jian-Wei Pan, o número mínimo de q-bits necessário para correção de erro quântico universal.
- 2009 — Yale criou o primeiro processador quântico de estado sólido, um chip supercondutor de 2 q-bit.
- 2011 — Cientistas da Austrália e do Japão fizeram um grande avanço no teletransporte quântico, transferindo dados quânticos com total integridade de transmissão. A D-Wave anunciou o primeiro recozedor quântico comercial.

- 2012 — O primeiro teletransporte quântico de um objeto macroscópico para outro foi relatado por cientistas da Universidade de Ciência e Tecnologia da China.
- 2013 — O Google anunciou que estava lançando o Quantum AI Lab.
- 2014 — Edward Snowden mostrou que a NSA está executando um programa de pesquisa de 79,7 milhões de dólares intitulado *Penetrating Hard Targets*, para desenvolver um computador quântico capaz de quebrar a criptografia vulnerável.
- 2015 — A NASA exibiu publicamente o primeiro computador quântico totalmente operacional do mundo, D-Wave Systems.
- 2016 — A IBM Research anunciou que, pela primeira vez, está disponibilizando a computação quântica ao público por meio da nuvem.
- 2017 — A IBM anunciou uma iniciativa pioneira no setor, chamada IBM Q, para construir sistemas de computação quântica universal disponíveis comercialmente. IBM, Intel e Google relataram testar processadores quânticos contendo 50, 49 e 72 q-bits.
- 2018 — Intel começou a testar um processador spin-q-bit baseado em silício. IonQ relatou que sua máquina poderia ser construída com 160 q-bits.
- 2019 — O Google anunciou que alcançou a supremacia quântica - marcando um grande marco no avanço da computação quântica prática. A IBM revela seu primeiro computador quântico comercial, o IBM Q System One.
- 2020 — Pesquisadores chineses afirmam ter alcançado a supremacia quântica, usando um sistema de 76 q-bit de pico fotônico (média de 43) conhecido como Jiuzhang, que realizou cálculos a 100 trilhões de vezes a velocidade dos supercomputadores clássicos.
- 2021 — Pesquisadores chineses relatam que construíram a maior rede de comunicação quântica integrada do mundo, combinando mais de 700 fibras ópticas com dois links QKD-terra-satélite para uma distância total entre nós da rede de redes de até 4.600 km.

[4] [6]

3 Máquina de Turing Quântica

3.1 Descrição de uma máquina de turing

O processo computacional foi graficamente mostrado por Turing que considerou um dispositivo que pudesse ler e escrever símbolos em uma fita que estava dividida em quadrados. Uma cabeça de leitura e gravação se moveria em qualquer direção ao longo da fita, um quadrado por vez, e uma unidade de controle poderia interpretar uma lista de instruções simples sobre leitura e gravação de símbolos nos quadrados, movendo-se, ou não, para a direita ou esquerda. O quadrado que é "lido"em cada etapa é conhecido como "quadrado ativo". A regra que está sendo executada determina o que se convencionou chamar estado da máquina. A fita é potencialmente infinita.

Cada instrução estabelece uma ação a ser executada. No caso, são estabelecidos quatro diferentes tipos de regra:

- Substituir branco por símbolo;
- Substituir símbolo por branco;
- Mover um quadrado para a direita;
- Mover um quadrado para a esquerda.

A máquina recebe um conjunto de instruções e executa. O dispositivo pode mover a cabeça de leitura e gravação para a direita ou esquerda, ler a posição, substituir um branco por símbolo, símbolo por branco ou apenas mover a cabeça novamente.

3.2 Lei de Moore

Gordon Earl Moore, tornou-se cofundador e presidente da Intel e constatou que a complexidade para construção de componentes (transistores), a um custo mínimo, tem aumentado aproximadamente um fator a cada dois anos. Em outras palavras, o número de transistores dos chips tem um aumento de 100%, pelo mesmo custo, a cada período de 2 anos. Essa previsão ficou conhecida com a Lei de Moore que mais tarde foi revista para um período que seria a cada 18 meses. [3]

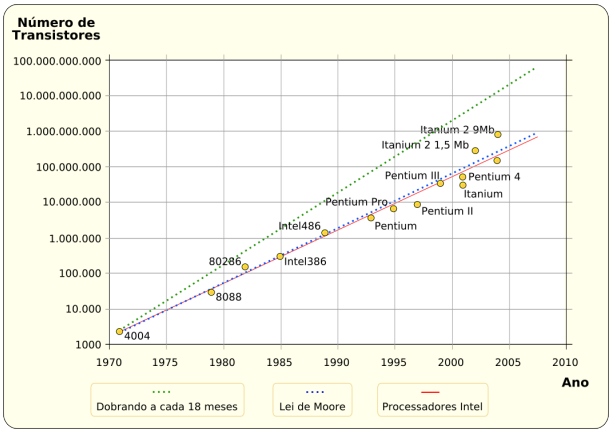

Figura 3.2: Gráfico da evolução dos transistores

Inicialmente a lei de Moore não passava de uma observação, mas acabou tornando-se um objetivo para as indústrias de semicondutores, fazendo-as despenderem muitos recursos para poder alcançar as previsões de Moore no nível de desempenho e é isso que torna a Lei de Moore realmente importante, pois sem ela, talvez não tivéssemos um desenvolvimento tão acelerado em nível de hardware e com custos cada vez mais acessíveis.

A indústria de semicondutores teve de investir em Pesquisa & Desenvolvimento, além de testes dos novos chips fazendo com que houvesse a formulação de uma "segunda Lei de Moore" onde era previsto um aumento no custo dos chips seguindo o aumento do desempenho, haja vista que a indústria de chips depende diretamente do custo de commodities como petróleo.

Em 2020 a lei de Moore previa que cada bit seria representado por apenas um átomo. Nesse limite, a computação passaria a ser regida pelas leis da mecânica quântica. [2]

3.3 Máquina de Turing Quântica

David Deutsch cria o primeiro algoritmo quântico em 1985, e faz uma descrição do equivalente quântico para a máquina de turing.

As funções realizadas em uma máquina de Turing Quântica ocorrem via interações quânticas. A fita e a cabeça em si existem em um estado quântico. No lugar da célula, a máquina de Turing Quântica abriga os q-bits, que apresentam estados de superposição de 0 ou 1. Ela pode codificar muitas entradas para um problema simultaneamente e calcular todas as entradas ao mesmo tempo.

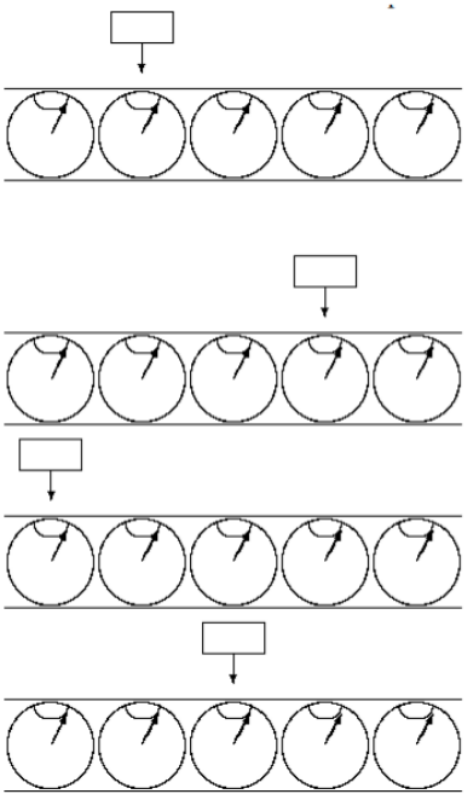

Figura 3.3: Esquema de uma Máquina de Turing Quântica.

Observa-se na figura 3.3 o primeiro esquema representando o estado inicial da fita e da cabeça. Os desenhos seguintes representam as posições diferentes que a cabeça se movimentam, podendo apresentar um estado superposto desses três estados ao mesmo tempo.

4 Bits x Q-bits

A unidade de informação clássica é o bit. Um bit pode ter os valores lógicos "0" ou "1". Nos computadores, bits são fisicamente representados pela presença ou não de correntes elétricas em componentes eletrônicos dentro dos chips: a presença da corrente indica o estado lógico 1 e a sua ausência o estado lógico 0. Obviamente que os dois valores lógicos de um bit clássico são mutuamente excludentes.

Analogamente, a unidade de informação quântica é o bit quântico,

ou q-bit (quantum-bit). Um q-bit pode ter os valores lógicos “0”, “1” ou qualquer superposição deles. Fisicamente, q-bits são representados por qualquer objeto quântico que possua dois autoestados bem distintos. Os exemplos mais comuns são: estados de polarização de um fóton (horizontal ou vertical), elétrons em átomos de dois níveis (o que é uma aproximação), elétrons em poços quânticos, e spins nucleares.
Um q-bit é um estado quântico da forma:

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

Os autoestados de um q-bit são representados pelos seguintes kets:

$$|0\rangle = \binom{1}{0} \quad ; \quad |1\rangle = \binom{1}{0}$$

5 Mecânica Quântica

5.1 Superposição

A computação quântica, assim como a clássica, se utiliza de uma unidade fundamental para trabalhar, o q-bit. O q-bit possui um estado associado $|\psi\rangle$ que pode ser qualquer vetor unitário dentro do espaço vetorial bidimensional abrangido por $|0\rangle$ e $|1\rangle$ sobre os números complexos. O q-bit será apresentado com mais detalhes no próxima capítulo.

Definição: Superposição é o fenômeno que permite um sistema quântico, não medido, estar em dois ou mais estados simultaneamente. Isto significa que um registrador quântico de n q-bits pode armazenar 2 n valores simultaneamente. Quando uma medida é realizada, o estado que antes estava em superposição colapsa para um único estado, e os demais se perdem. Portanto, pode-se dizer que um q-bit pode estar em superposição em tempo de execução, pois quando é realizada uma medida, o valor deste se colapsa para um dos estados ($|0\rangle$ ou $|1\rangle$) com a probabilidade de cada um dos estados.

5.2 Emaranhamento

Definição: O emaranhamento (ou entrelaçamento) quântico é o fenômeno que ocorre quando pares ou grupos de partículas interagem de forma que o estado quântico de cada uma não pode ser descrito independentemente, e ao invés disso, um estado quântico deve ser dado para o sistema como um todo. O entrelaçamento acontece quando duas partículas continuam se influenciando separadas, por qualquer distância. O que acontece em uma

partícula é refletido na outra. Por exemplo, um spin no sentido horário na primeira partícula será equivalente a um spin no sentido anti-horário na segunda, além disso, o spin combinado será zero. [5]

5.3 Teorema da Não-Clonagem

Não existe uma transformação que clona, ou que copia, sem prejuízo o estado de um q-bit qualquer para outro. Para clonar um estado é necessário realizar uma medição, entretanto, ao realizar a medição pode-se ter criado um q-bit clone, mas o q-bit original irá colapsar. Teorema (Não-clonagem) Seja H um espaço de Hilbert. Então não existe uma transformação $\mathcal{U} : \mathcal{H} \otimes \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}$ tal que exista um $|s\rangle$, satisfazendo para qualquer $|\psi\rangle$:

$$\mathcal{U}(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$$

6 Portas Lógicas Quânticas

6.1 Porta CNOT Quântica

A Porta CNOT atua em estados de 2 q-bits de entrada, o controle e o alvo. Uma porta controlada age de acordo com o q-bit de controle. Ela será ativada apenas quando o q-bit de controle estiver no estado $|1\rangle$. Os q-bits de controle e alvo podem ser estados superpostos, além disso, podem estar emaranhados. [1]
A representação matricial da porta quântica CNOT é a dada por:

$$CNOT = \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix}$$

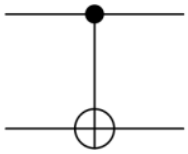

Figura 6.1: Representação circuital da Porta CNOT Quântica. A linha superior representa o q-bit de controle, e a linha de baixo o q-bit-alvo

6.2 Porta Toffoli Quântica

O funcionamento da porta Toffoli é bastante semelhante a CNOT, também é uma porta controlada, só que com dois q-bits de controle. Seu funcionamento pode ser da seguinte maneira, caso os q-bits $|a\rangle$ e $|b\rangle$ sejam iguais a $|1\rangle$ o q-bit $|c\rangle$ será negado.
A representação matricial da porta Toffoli é dada por:

$$TOFFOLI = \begin{bmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000001 \\ 00000010 \end{bmatrix}$$

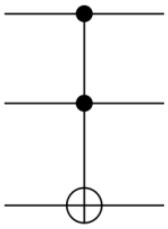

Figura 6.2: Representação circuital da Porta Toffoli Quântica. As linhas superiores representam os q-bits de controle, e a linha de baixo o q-bit-alvo.

6.3 Porta Swap

A porta de Swap, como pode ser visualizado na figura 6.3, é formado por três portas CNOT.
A evolução desta porta pode ser descrita como a troca de seus valores entre si.
A representação matricial da porta Swap é dada por:

$$SWAP = \begin{bmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{bmatrix}$$

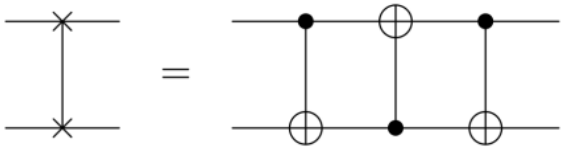

Figura 6.3: Representação circuital da Porta Swap Quântica.

6.4 Porta Fredkin

A porta Fredkin, que também é uma porta controlada, funciona com um q-bit de controle associado à uma porta Swap. Seu funcionamento pode ser da seguinte maneira, caso o q-bit de controle seja $|1\rangle$ e os q-bits alvo trocam de valor entre si.
A repreesntação matricial da porta Fredkin é dada por:

$$FREDKIN = \begin{bmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000010 \\ 00000100 \\ 00000001 \end{bmatrix}$$

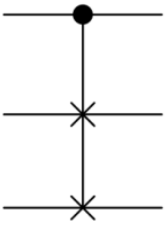

Figura 6.4: Representação circuital da Porta Fredkin Quântica. A linha superiore representam o q-bit de controle, e as linha de baixo os q-bits-alvo.

6.5 Porta U_f ou Oráculo

É uma porta muitas vezes chamada de *black box*. É uma porta que não é pré-definida e, portanto, pode ser utilizada para manipular qualquer número de q-bits. Em outras palavras, ela é uma porta "genérica" onde se pode implementar qualquer operação, desde que esta obedeça às regras dos operadores unitários.
São operadores lineares unitários que calculam uma função característica arbitrária e desconhecida.
Oráculos são amplamente utilizados em algoritmos quânticos voltados para problemas de busca ou extração de informações de funções desconhecidas.

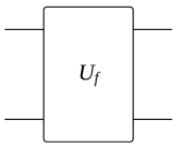

Figura 6.5: Representação circuital de uma Porta Oráculo.

7 Conclusão

A Computação Quântica é um campo emergente de pesquisa na interseção de ciência da computação na 4ª revolução industrial. Ela pode ser usada para diversas funcionalidades, tais como: aplicações em criptografia, simulação de sistemas mecânicos quânticos complexos, inteligência artificial, previsão do tempo, etc. Os computadores quânticos serão indispensáveis no futuro. Nos últimos anos, houve imenso progresso com experiências de Computação Quântica com o IBM Quantum Experience (IBM QE), onde os computadores quânticos reais estão ao alcance de qualquer pessoa.

O principal objetivo da computação quântica é a realização de operações lógicas usando portas quânticas que evitem a propagação de erros entre os q-bits físicos. A construção de portas quânticas usando o teleporte quântico, oferece um valioso recurso a computaçãoo quântica, pois possibilita realizar experiências a sua implementação física.

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 também 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 consequências, 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.

O estudo da computação quântica mostra-se de grande importância nos dias atuais. Isso se deve a capacidade dessa teoria revolucionar o mundo da computação. Tendo isso em mente, a pesquisa nesta área mostra-se de suma importância para o desenvolvimento das tecnologias atuais e futuras.

Bibliografia

[1] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge Press, 2001).

[2] I. Oliveira, A revolução dos Q-bits (Zahar, 2017)

[3] https://pt.wikipedia.org/wiki/Computaç~ao_quântica

[4] https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication

[5] W. J. N. Silva, Uma introdução à Computação Quântica (2018) https://www.ime.usp.br/~map/tcc/2018/WagnerJorcuvichV3.pdf

[6] https://www.quthought.com/post/history-of-quantum-computing-a-timeline