# Introdução à Computação Quântica

Tony Minoru Tamura Lopes
Instituto de Computação - UNICAMP
Avenida Albert Einstein, 1251
Campinas, Brasil
ra017502@students.ic.unicamp.br

## RESUMO

A incessante busca por aumento na eficiência de processamento chegará a seu limite quando poucos átomos forem necessários para representar um bit. Quando isso acontecer, a Computação Quântica entrará em voga. Ela, além de permitir a construção de chips minúsculos, fornecerá novas bases para a computação, permitindo a realização de tarefas impossíveis na computação utilizada atualmente. Para compreender isso, serão introduzidos neste trabalho, a unidade básica de informação quântica, o Qubit, e os diversos fenômenos quânticos necessários na obtenção de novos limitantes inferiores para problemas conhecidos. Será detalhada a aplicação mais notável da Computação Quântica, que é a fatoração de números inteiros em tempo polinomial, a qual por sua vez têm implicações diretas na segurança em comunicações. Em contrapartida a isso, um modo totalmente novo e seguro de comunicar-se será descrito utilizando de canais quânticos de informação. Todas essas aplicações já possuem implementações reais, mostrando que a Computação Quântica tem, além de modelos matemáticos concisos, possíveis vantagens práticas sobre a Computação Clássica.

## Categorias e Assuntos

A.1 [**INTRODUCTORY AND SURVEY**]: Computação Quântica

## Termos Gerais

Teoria

## Palavras Chaves

Computador Quântico, Algoritmos Quânticos, Informação Quântica, Criptografia Quântica, Qubit

## 1. INTRODUÇÃO

*"A informação, a transmissão de informação e o processamento de informações são governadas por fenômenos físicos"*. Como veremos, essa simples afirmação possui implicações nada triviais para a computação.

Em toda sua história, o computador foi implementado de diversas maneiras, utilizando desde engrenagens, relês e válvulas, chegando mais atualmente aos transistores, circuitos integrados e chips. Todas essas maneiras de construir um computador baseiam-se em leis da física e, portanto, são nada mais do que experimentos físicos em princípio.

Nos últimos 40 anos ocorreram reduções dramáticas nas dimensões dos chips em busca de mais eficiência no armazenamento de memória e velocidade de processamento. Ao passo do desenvolvimento tecnológico atual, chegaremos rapidamente à necessidade de poucos átomos para representar-se um bit. Quando isso acontecer, as leis que governarão os fenomenos físicos serão as da Quântica.

A física Quântica, por outro lado, fornecerá muito mais do que a possibilidade de miniaturização dos chips, ela fornecerá uma revolução nas bases da computação, entendendo a classe de problemas tratáveis e permitindo novos limitantes inferiores para algoritmos. Hoje, alguns resultados já demonstram que computadores quânticos podem realizar a fatoração de inteiros em tempo polinomial. Essa habilidade é de extremo impacto, já que muito da segurança em comunicações baseia-se na intratabilidade deste problema.

Em contrapartida, ao fato de tornar os sistemas de comunicação inseguros, a Quântica fornece um meio totalmente seguro de comunicar-se. É possível, através de canais quânticos, criar uma chave privada compartilhada, com garantias de que ela só é conhecida pelas partes comunicantes.

Para compreender como esses avanços serão possíveis, a seção 2 fará uma análise das bases da computação, enquanto a seção 3 mostrará onde a Computação Quântica realizará suas modificações. As seções 4 e 5 discorrerão sobre os principais fenômenos quânticos e quais objetos úteis à computação, eles fornecerão. Além disso, serão detalhados os modelos matemáticos que explicam os fenômenos e alguns experimentos utilizados para identificá-los. Em seguida, a seção 6 apresentará o modelo de um computador quântico completo. Com este modelo, poderão ser introduzidos alguns algoritmos quânticos e a Comunicação Quântica segura, na seção 7. Por fim, as seções 8 e 9 mostrarão respectivamente, o estado atual da implementação de computadores quânticos reais e uma conclusão final.

## 2. INICIO DA COMPUTAÇÃO

Em 1900, o matemático alemão David Hilbert propôs 100 problemas, os quais sobre sua perspectiva seriam os grandes desafios daquele século. Um deles era o *Entscheidungspro-*

*blem*, ou "Problema de Decisão", que questionava se existiria um procedimento mecânico para determinar a veracidade de qualquer conjectura ou questão matemática. Para responder a esse problema, Alan Turing descreveu o que conhecemos como "Máquina de Turing" ou "Máquina Determinística de Turing".

A "Máquina de Turing" consistia de uma fita unidimensional de dados e uma cabeça deslizante de leitura e escrita (Figura 1). A cabeça possuía um estado interno e um conjunto de instruções, as quais diziam, sobre o estado interno da cabeça, qual direção ela devia deslizar, qual o seu próximo estado e o que devia ser escrito na fita.

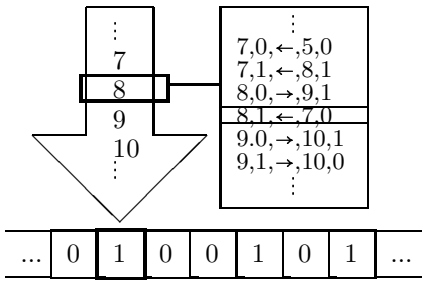


**Figura 1: Uma Máquina Determinística de Turing. Nela, a flecha representa a cabeça de escrita e leitura com seu estado atual assinalado. Na caixa ao lado estão as instruções.**

Esse mecanismo resolvia o *Entscheidungsproblem*, demonstrando não haver um procedimento mecânico capaz de decidir a veracidade de todos as conjecturas ou questões matemáticas. Um exemplo clássico de problema indecidível está em determinar se a máquina termina de executar para um conjunto de estados iniciais qualquer. Por outro lado, essa máquina possuía o mesmo poder de fornecer provas da própria matemática e, portanto, a matemática também era incompleta[5].

Não levando-se em conta alguns problemas ditos *indecidíveis*, a máquina proposta ainda representava um grande avanço, pois solidificava o conceito da computação. De fato, como modelo matemático, essa máquina fundamentou os computadores atuais. A máquina em si, nunca foi implementada comercialmente, mas sua simplicidade foi útil para o desenvolvimento da Teoria da Computação, já que qualquer teorema provado sobre ela é válido para todos as implementações de computadores.

No entanto, na época do desenvolvimento da Máquina de Turing, não estavam claras quais eram as suposições físicas intrínsecas no modelo matemático e quais seriam as implicações disso. Hoje, sabe-se que a Máquina de Turing sustenta-se, dentre outras, na suposição, de que os símbolos na cabeça de leitura e na fita existem unicamente em um dado momento e unidade de armazenamento, ou seja, uma região da fita pode conter 0 ou 1, em cada instante.

Essas suposições levantam a questão: A máquina de Turing é uma boa abstração matemática, mas ela é consistente com a física conhecida? A resposta seria afirmativa na época de Turing, pois a compreensão da física até então não poderia implementar o armazenamento de informação de outra maneira. No entanto, a resposta torna-se negativa quando consideramos pequenas dimensões e os fenômenos são explicados pela Quântica.

# 3. COMPUTAÇÃO QUÂNTICA

A crescente miniaturização dos computadores, como forma primária para obtenção de mais eficiência computacional, irá alcançar seu limite por volta de 2020, conforme a lei de Moore, com os processadores operando a cerca 40GHz. Neste ponto, serão necessários poucos átomos para representar um bit e as leis da Quântica serão as válidas.

É notável que os ganhos em utilizar efeitos quânticos em um computador não serão somente para viabilizar chips ainda mais minúsculos. Os fenômenos quânticos permitirão uma revolução no paradigma primordial da computação e proverão ganhos, em certas aplicações, nunca alcançáveis por computadores clássicos mesmo em paralelo.

Nesse contexto, David Deutsch em 1985, apresentou a "Máquina Quântica de Turing" em continuidade ao trabalhos de Richard Feynman. Essa máquina diferenciava-se inicialmente por ser reversível, ou seja, é possível da entrada obter a saída e vice-versa. Um exemplo de computação irreversível é a porta lógica AND, na qual a saída 0 não determina sua entrada. Essa reversibilidade é necessária em sistemas quânticos. No entanto, os dois pontos mais contrastantes nesse novo modelo, eram a possibilidade de armazenamento de 0, 1, ou ambos ao mesmo tempo, e o processamento de todos os caminhos possíveis em paralelo pela cabeça da máquina. Apesar desses fenômenos fugirem ao senso comum, e de fato não são explicáveis pela física clássica, eles são perfeitamente descritos pela física Quântica.

O primeiro ganho da "Máquina Quântica de Turing" sobre a "Máquina Determinística de Turing" é a possibilidade de simular sistemas quânticos de maneira eficiente. Atualmente, há argumentos fortes mostrando a necessidade de uma carga exponencial para "Máquina Determinística de Turing" simular esses sistemas, e conseqüentemente, os computadores atuais herdam essa ineficiência.

Nas próximas seções serão descritos os componentes necessários à construção de um computador Quântico que seja equivalente a uma "Máquina Quântica de Turing".

# 4. SUPERPOSIÇÃO E INTERFERÊNCIA

A melhor maneira de explicar a *superposição* e a *interferência*, os dois fenômenos principais para a Computação Quântica, é visualizar o experimento das duas fendas[1]. Nesse experimento, um canhão de elétrons é posicionado à frente de um anteparo com duas fendas e atrás do anteparo é colocado um detector de elétrons, conforme a Figura 2.

Caso uma das fendas seja deixada fechada, encontraremos no dectetor os padrões da Figura 2.a e 2.b. A explicação para esses padrões vêm do comportamento dual, onde partículas atômicas comportam-se ou como ondas ou como partículas em diferentes condições. Outra configuração para o experimento é quando as duas fendas estão abertas apresentando o padrão da Figura 2.c. Esse padrão é descrito pela *interferência* entre ondas.

Até aqui, existem explicações plausíveis pela física clássica para todos os resultados obtidos. O problema começa quando realizamos a emissão de um elétron por vez. Como o elétron pode passar por somente uma das fendas, não seria possível a interferência. No entanto, o resultado do experimento diz o contrário, como se o elétron interferisse consigo mesmo. O único modo de explicar esse comportamento é através da

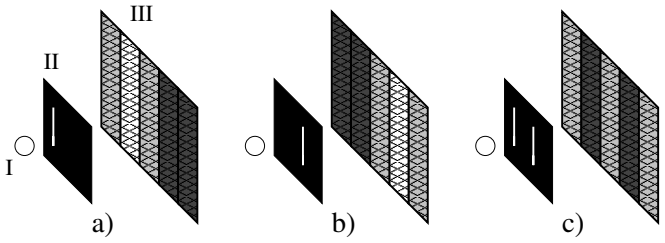


**Figura 2: O ítem I é o emissor de elétrons. II é o anteparo com fendas e III o anteparo detector. Em a) e b) só uma das fendas estão abertas. Com as duas fendas abertas em c) percebe-se a *interferência***

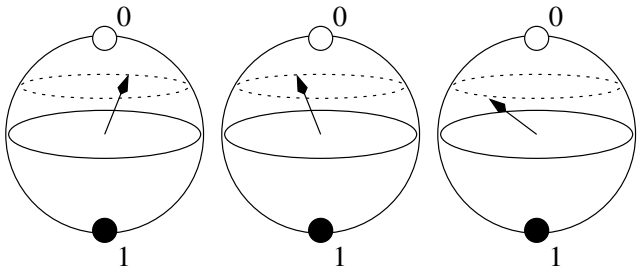


**Figura 3: Três Qubits com mesmas probabilidades de obtenção de 0's ou 1's, porém, com fases diferentes**

física Quântica.

## 4.1 Estado Quântico

Uma pergunta natural, sobre o experimento das duas fendas com uma partícula por vez, é "qual das duas fendas o elétron passou?". A explicação quântica para o experimento impede que responda-se a essa pergunta e ainda obtenha-se o padrão de *interferência*. Na verdade, a passagem do elétron por uma das fendas configura um estado quântico condicionado ao princípio da incerteza de Heisenberg[3]. Ou seja, para determinar a fenda devemos entrar em contato com a partícula e o efeito quântico não ocorrerá, pois houve decoerência.

Para compreender o que ocorre com o elétron, não devemos interagir com o sistema, mas podemos prever seu comportamento através de probabilidades. É nesse momento que introduziremos a notação **BraKet** ($\langle . || . \rangle$) de Dirac[3], originalmente utilizada em probabilidade condicional. Utilizaremos somente o **Ket** ($|.\rangle$) , que representa os eventos finais ou estados quânticos.

No caso do experimento, os eventos finais ou estados quânticos são "passou pela fenda 1", "passou pela fenda 2" ou uma *sobreposição* de ambos com diferentes probabilidades. Para poder representar todas as possibilidades de *sobreposição* devemos utilizar espaços de Hilbert ou, mais especificamente, *espaços vetoriais complexos de dimensão finita*.

O estado quântico $|\psi\rangle$, dizendo qual fenda o elétron passou, é representado neste caso como:

$$|\psi\rangle = c_0|\text{passa pela fenda 1}\rangle + c_1|\text{passa pela fenda 2}\rangle \qquad (1)$$

onde $c_0 = c_1 = \frac{1}{\sqrt{2}}$, e $|c_0|^2 + |c_1|^2 = 1$, pois $|c_0|^2$ e $|c_1|^2$ são as probabilidades de passar em cada uma das fendas. Como deve-se passar por alguma delas, o somatório das probabilidades é 1 (100%). Os termos $|\text{passa pela fenda 1}\rangle$ e $|\text{passa pela fenda 2}\rangle$ são bases ortogonais do espaço vetorial e os dois únicos valores possíveis de obter-se em uma medição.

Sendo assim, somos tentados a dizer que, portanto, a partícula passa pelas duas fendas em diferentes proporções e essas diferentes proporções interferem entre si. Na realidade, a partícula é uma entidade localizada e só podemos dizer sobre a probabilidade dela passar em cada uma das fendas. Entretanto, esse último argumento não explica a interferência. Na realidade, o comportamento resultante da *interferência* é condicionado pela simples probabilidade do elétron passar por cada uma das fendas e, portanto, o elétron realmente interfere consigo mesmo.

A utilização de elétron nesse experimento não é determinante para o comportamento obtido. Outras partículas atômicas, como prótons, nêutrons e até os próprios atomos já foram utilizados e obtiveram o mesmo resultado[2]. O estado quântico neste experimento também não é o único existente. O spin de um núcleo, o nível energético de um elétron e até mesmo a polarização do fóton são estados quânticos e obedecem as mesmas leis quânticas apresentadas.

## 4.2 Qubit

A unidade fundamental de informação clássica é o bit. Ele é caracterizado por uma chave com dois estados "desligado" ou 0 e "ligado" ou 1. A implementação física de um bit requer um dispositivo com dois estados possíveis, onde exista uma barreira forte o suficiente para impedir uma transição de estados, a não ser quando desejado.

O análogo quântico para o bit é o Qubit ou Quantum Bit, este também possui dois estados, porém quânticos, designados por $|0\rangle$ e $|1\rangle$. Teoricamente, qualquer sistema quântico que possua dois estados possíveis pode implementar um Qubit. Assim, denotamos o estado genérico de um Qubit como:

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (2)$$

onde $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$. O que significa que o Qubit pode ter qualquer valor entre 0 e 1, e se realizarmos uma medição, ele tem probabilidade $|\alpha|^2$ de ficar em 0 e $|\beta|^2$ de ficar em 1. A Figura 3 mostra a representação gráfica de um Qubit. Os valores possíveis são todos aqueles na superfície da esfera apontados pela flecha, denotando a *fase* do Qubit. Essa forma é obtida por que os coeficientes são números complexos e a soma dos quadrados de suas normas resulta em 1.

A Figura 3 também ilustra três Qubits com mesma probabilidade de medir-se 0 e 1, porém com *fases* diferentes. Essa diferenças de fase acontecem, pois $|\alpha|^2 = |-\alpha|^2$. Apesar dessa propriedade ser inócua na perspectiva de medição, onde só importa a probabilidade, em computadores quânticos, os algoritmos funcionam através de transformações em Qubits, alterando os coeficientes complexos controladamente. Ou seja, trabalhamos com um vetor de entrada $In = (\alpha\,\beta)^T$ e temos $Out = XIn = (\alpha'\,\beta')^T$ após a aplicação de uma transformação $X$ unitária, ou seja, uma bijeção do espaço original a ele mesmo.

# 5. MÚLTIPLOS QUBITS E PARALELISMO

Ao construir um computador quântico ou mesmo para a "Máquina Quântica de Turing" precisamos lidar com mais

de um Qubit. Análogamente à computação clássica, podemos criar um *registrador quântico*. No entanto, enquanto que em um registrador clássico de $n$ bits podemos ter qualquer número de 0 até $2^n$, mas somente um desses números por vez, em um *registrador quântico* podemos ter uma *superposição* de todos eles.

Um exemplo de estado quântico para um registrador de 3 Qubits seria:

$$|\psi\rangle = c_0|0\rangle|0\rangle|0\rangle + c_1|0\rangle|0\rangle|1\rangle + c_2|0\rangle|1\rangle|0\rangle + \cdots + c_7|1\rangle|1\rangle|1\rangle \quad (3)$$

ou ainda, na base decimal:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle + \cdots + c_6|6\rangle + c_7|7\rangle \quad (4)$$

onde $|c_0|^2 + |c_1|^2 + \cdots + |c_7|^2 = 1$. Isso significa que podemos ter todos esses números ao mesmo tempo dentro de um registrador. Dessa forma, a capacidade de lidar com informação é exponencialmente maior se comparado ao modo clássico. É claro que, ao realizarmos uma medição somente um dos $2^n$ números será visto. Isto aparentemente nos leva a concluir que afinal não existem ganhos reais em um *registrador quântico*. Entretanto, é nesse momento que introduzimos o *paralelismo quântico*, a habilidade especial que faltava para concluir a "Máquina Quântica de Turing".

O *paralelismo quântico* acontece quando realizam-se operações em um *registrador quântico* em estado de *superposição*. Quando isso ocorre, a operação é realizada sobre todos os valores superpostos, conseqüência direta da *interferência*, e obtém-se com isso um ganho exponencial de tempo. Já que não podemos obter todos os resultados dessa operação ao realizar uma medição, devemos aplicar as operações de forma que somente as respostas válidas possuam probabilidades altas e seja possível recuperá-las após um tempo previsto.

## 5.1 Qubits emaranhados e não-Localidade

Uma outra forma mais interessante de apresentação de múltiplos Qubits é quando estes estão *emaranhados*. Para compreender esse fenômeno, imagine um par de partículas emitidos de uma fonte em sentidos opostos do mesmo eixo (Figura 4). Caso a partícula 1 esteja no raio apontando para cima, a partícula 2 estará no raio apontando para abaixo e vice-versa. Sendo assim, após a emissão das partículas, o estado quântico do sistema é:

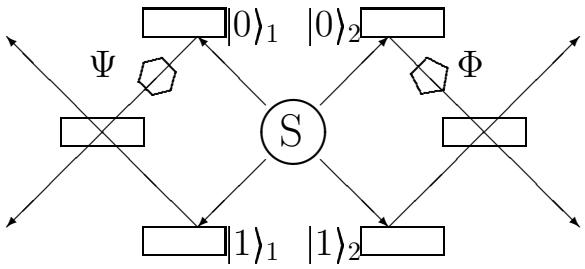


**Figura 4: A fonte de S emite duas partículas em sentidos opostos de um mesmo eixo. Assim, ao medir-se o estado quântico de uma partícula saberemos exatamente o estado da outra, pois elas estão *emaranhadas*.**

$$|Q\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right) \quad (5)$$

Veja que neste estado quântico não possuímos todas bases possíveis com dois Qubits normais. Isso acontece por que quando os Qubits estão *emaranhados*, o estado quântico de um Qubit implica no estado quântico do outro. No caso desse experimento, o fato de serem emitidos em sentidos opostos, implica que ao medir-se o primeiro Qubit já concluiremos com certeza a condição do outro sem necessidade de medição.

Por outro lado, o resultado mais interessante desse fenômeno acontece após a aplicação de diferentes rotações Ψ e Φ nas fases das partículas. Feito isso, ao realizar certas medições, não é possível explicar os parâmetros obtidos em uma partícula sem considerar a transformação realizada na outra partícula!

Esse fenômeno é conhecido como *não-localidade* e a influência é detectada independentemente da distância entre as partículas, sugerindo uma interação não-local entre elas. Apesar de cientistas como Einstein, Podolsky e Rosen[6] argumentarem filosoficamente que existiria uma "variável escondida" ligando as partículas e realizando a interação local, Jonh Bell demonstrou matematicamente a inconsistência desse argumento, evidenciando a *não-localidade*.

## 5.2 O ciclo Preparar-Evoluir-Medir

Um computador clássico opera em um ciclo de **Carregar-Executar-Gravar**, já um computador quântico opera no ciclo **Preparar-Evoluir-Medir**. A etapa de preparação consiste em inicializar o *registrador quântico* em um estado qualquer, como por exemplo uma superposição de todos os números com igual probabilidade de medição. Após isso, é necessário aplicar um conjunto de operações reversíveis, que como dito anteriormente, são transformações nos coeficientes complexos dos Qubits. Por fim, deve-se medir o resultado obtido após um tempo determinado.

Em uma "Máquina Quântica de Turing" este ciclo faria com que todas as decisões fossem tomadas entre o estado inicial até o momento da medição, através do *paralelismo quântico*. Deve-se, portanto, implementar essas operações de forma que todos os caminhos levem no momento da medição às respostas do problema. Outra implicação desse ciclo, é incapacidade de uma "Máquina Determinística de Turing" eficientemente simular a fase de evolução com todo seu paralelismo ou armazenar em sua memória um estado de superposição preparado inicialmente.

Não há, entretanto, ganhos em computabilidade. A classe dos problemas *indecidíveis* é inalterada sobre a perspectiva Quântica em relação à clássica. Os ganhos estão em complexidade, sendo possíveis novos limitantes inferiores inalcançáveis anteriormente.

Da mesma forma que a versão clássica determinística, a "Máquina Quântica de Turing" é um modelo matemático útil para provar teoremas sobre Computação Quântica. Há também a implementação lógica deste conceito matemático, a qual é base para a construção de um computador quântico real. Nas próximas seções, serão discutidos os componentes básicos para implementá-lo e com isso será possível definir algoritmos quânticos.

# 6. PORTAS QUÂNTICAS E CIRCUITOS QUÂNTICOS

Para a construção de computador quântico, ou mesmo para a descrição de um algoritmo, é necessária a definição de elementos básicos sobre os quais seja possível criar qualquer outra operação. Em um computador clássico, as portas lógicas AND, NOT e a ligação delas através de suas entradas e saídas são suficientes para executar qualquer algoritmo ou mesmo construir um computador genérico nos moldes de Von Neunman. Para os computadores quânticos, precisamos das portas lógicas quânticas de Rotação de 1-Qubit (um conjunto infinito de portas) e NOT-Controlado, detalhadas a seguir, e que cada uma dessas portas sejam reversíveis. Além disso, a ligação entre as portas deve transferir estados quânticos em *superposição*.

## 6.1 Rotação de 1-Qubit

Como foi dito anteriormente, transformações sobre Qubits são alterações nos coeficientes complexos de suas bases. Além disso, no caso de um Qubit essa alteração representa uma rotação da fase, levando na representação em esfera (Figura 3) de um ponto da superfície a outro. Uma porta lógica quântica de rotação de 1-Qubit pode ser construída para realizar uma rotação arbitrária. Como existe um número infinito de rotações possíveis, existem infinitas portas de rotação de 1-Qubit que podem ser definidas.

Um exemplo é a porta "Raiz-Quadrada-do-NOT" ($\sqrt{\text{NOT}}$), a qual recebe uma entrada e fornece uma saída. Se colocadas duas dessas portas encadeadas temos a operação NOT. Como $\sqrt{\text{NOT}}$ trata-se de uma transformação, só é necessário defini-la sobre as bases do espaço vetorial para ter o resultado sobre qualquer outro ponto do espaço:

$$U_{\sqrt{\text{NOT}}}|0\rangle = \left(\frac{1}{2} + \frac{i}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{i}{2}\right)|1\rangle$$
$$U_{\sqrt{\text{NOT}}}|1\rangle = \left(\frac{1}{2} - \frac{i}{2}\right)|0\rangle + \left(\frac{1}{2} + \frac{i}{2}\right)|1\rangle$$

E para a operação NOT:

$$\text{NOT}|0\rangle = U_{\sqrt{\text{NOT}}}U_{\sqrt{\text{NOT}}}|0\rangle = |1\rangle$$
$$\text{NOT}|1\rangle = U_{\sqrt{\text{NOT}}}U_{\sqrt{\text{NOT}}}|1\rangle = |0\rangle$$

Uma outra porta de rotação 1-Qubit muito importante é a de Walsh-Hadamard, definida como:

$$U_{\text{WH}}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$U_{\text{WH}}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Essa porta, se aplicada a um Qubit com $|0\rangle$, leva ao meio do caminho até $|1\rangle$ e vice-versa. Nestes casos, a probabilidade de obter 0 ou 1 em uma medição será de 50% para cada.

A porta de Walsh-Hadamard é muito utilizada em algoritmos quânticos para, a partir de um registrador quântico com $n$ Qubits, deixá-los todos em estado de superposição, com o registrador possuindo os $2^n$ valores possíveis com igual probabilidade de serem medidos.

## 6.2 NOT-Controlado

Para conseguir alcançar qualquer tipo de Computação Quântica, só é necessário mais uma porta lógica em conjunto às de rotação de 1-Qubit, a porta NOT-Controlado ou CN, definida como:

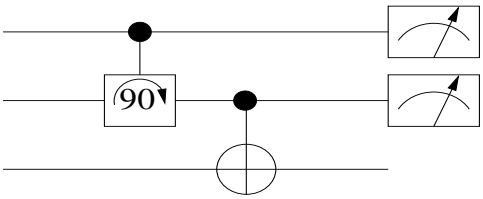


**Figura 5: Exemplo de um circuito quântico com 3 Qubits de entrada, duas medições, uma porta de rotação e uma NOT-Controlado.**

$$U_{\text{CN}}|00\rangle = |00\rangle$$
$$U_{\text{CN}}|01\rangle = |01\rangle$$
$$U_{\text{CN}}|10\rangle = |11\rangle$$
$$U_{\text{CN}}|11\rangle = |10\rangle$$

CN é uma porta 2-Qubit que, basicamente, inverte o segundo Qubit caso o primeiro seja $|1\rangle$ e não altera-o, caso contrário. Deve-se notar que esta lógica condicional não envolve medições em momento algum.

A influência de um Qubit no outro, apresentado por esta porta, realiza a ligação necessária para criar circuitos quânticos e ainda pode ser utilizada para produzir estados *emaranhados*, extremamente úteis em algoritmos quânticos.

## 6.3 Circuitos Quânticos

A Figura 5 demonstra o esquema básico de um circuito quântico. Essa representação é independente de implementação física. Nela, as linhas horizontais representam a transferência de um estado quântico da esquerda para a direita. As linhas verticais, interligando duas horizontais, sincronizam as duas transferências.

A presença de um símbolo •, ligando um estado quântico a uma porta lógica, designa um controle desse estado quântico sobre a operação da porta lógica, similarmente ao CN. Durante as linhas horizontais, mas mais comumente ao fim delas, pode haver uma medição representada pelo símbolo da fase.

É comum a utilização de diagramas simplificados, onde há linhas horizontais com múltiplos Qubits e "caixa-pretas", que não possuem seu circuito interno mostrado.

# 7. ALGORITMOS QUÂNTICOS

A Computação Quântica fornece um novo paradigma para o processamento de informação e seu armazenamento. A grande questão é: Quais aplicações poderão tirar proveito de todo o seu potencial? A primeira grande resposta para essa pergunta, e que trouxe atenção e investimentos à Computação Quântica, foi a fatoração de inteiros. Enquanto, outras aplicações já demonstravam a obtenção de novos limitantes inferiores para algoritmos[5] ou mesmo a viabilidade de simulações quânticas, a fatoração de inteiros possuía implicações de proporções gigantescas.

## 7.1 Fatoração de Inteiros

Grande parte da segurança em comunicações baseia-se na utilização de chaves para encriptação e decriptação. O RSA

é um esquema muito famoso baseado em tal conceito. Nele, uma pessoa faz a distribuição em um canal inseguro de uma chave pública. Caso outra pessoa desejar comunicar-se, ela deve encriptar a mensagem com aquela chave. A impossibilidade de decriptação dos dados, senão por uma chave privada, cria um canal seguro de comunicação.

Para possibilitar a encriptação e decriptação, a construção dessas chaves utiliza, por exemplo, dois números primos grandes como fatores. Mesmo sendo possível, teoricamente, a partir da chave pública descobrir a chave privada, seria necessário realizar a fatoração de inteiros. A suposta intratabilidade desta tarefa garante a segurança das comunicações.

Não há provas de que a fatoração de inteiros seja um problema intratável classicamente. Mas, atualmente, o melhor algoritmo para a resolução do problema, o "Number Field Sieve", possui tempo de execução proporcional a $exp(cL^{1/3}log(L)^{2/3})$ onde $L$ é a quantidade de bits necessários para representar o número. A última conquista desse algoritmo foi a resolução do desafio RSA-640, onde o número original possuía 193 dígitos decimais. Para conseguir isso, foram necessários 80 processadores Opteron de 2.2Ghz e 3 meses de processamento.

Aparentemente, o paralelismo clássico pode ser usado intensamente para fatorar números mais desafiadores. Entretanto, pode-se afimar que: dado um número com 2000 dígitos para o algoritmo "Number Field Sieve", mesmo se cada átomo do universo fosse um computador clássico processando à máxima velocidade por toda a vida do universo, o esforço não seria suficiente para fatorar o número.

Essa incapacidade dos computadores clássicos pode ser resolvida caso seja encontrado um algoritmo polinomial para o problema, o que ainda não aconteceu. Neste caso, a Computação Quântica poderia fornecer algum ganho?

### 7.1.1 O Algoritmo de Shor

Em 1994, Peter Shor[4] descobriu um modo de fatorar inteiros utilizando um computador quântico em tempo polinomial. Para conseguir esse feito, ele necessitou principalmente de resultados anteriores sobre Transformadas Rápidas de Fourier, por Simon[1], e da relação entre o período de uma função periódica e os fatores de um número.

Devemos detalhar cada um desses resultados para compreender o Algoritmo de Shor.

#### 7.1.1.1 Teoria dos Números e Fatoração de Inteiros.

Tendo um número $n$ (o número a ser fatorado), definimos a função $f_n(a) = x^a \bmod n$, onde $x$ é relativamente primo a $n$, pois $mdc(x,n) = 1$. Sendo assim, essa função é periódica, ou seja, existe um $f_n(x+r) = f(x)$ e $r$ é o período da função. A teoria do números, diz que há grande probabilidade do $\mathrm{mdc}(x^{r/2}-1,n)$ ser um fator não-trivial de $n$, ou seja, diferente de 1 e do próprio $n$.

Para exemplificar, digamos que $n = 15$ e $x = 8$ escolhido aleatoriamente. Calculando $f_{15}(a) = 8^a \ mod\ 15$ para $a = \{0,1,2\dots\}$, temos a seqüencia $\{1,8,4,2,1,8,4,2,1,\dots\}$. Percebe-se rapidamente que $f_{15}(a+4) = f(a)$, portanto, $r = 4$. Finalmente, computando $\mathrm{mdc}(x^{r/2}-1,n)$, temos $\mathrm{mdc}(8^{4/2}-1,15) = \mathrm{mdc}(63,15) = 3$. De fato, 3 é um fator não-trivial de 15 e tendo este fator, é fácil descobrir o outro fator com $15/3 = 5$. Os dois fatores são, então, 3 e 5.

#### 7.1.1.2 Transformada Rápida de Fourier e Periodicidade.

A partir dos resultados anteriores, poderíamos chegar facilmente a um algoritmo probabilístico para fatorar inteiros. O único problema está em achar $f_n(x+r) = f(x)$, o qual necessitaria $O(2^L)$ tentativas em um computador clássico, onde $L$ é a quantidade de bits necessários para representar o número $n$. Usando quântica conseguimos calcular $r$ com somente $O(L^2)$ passos, representando uma aceleração exponencial neste algoritmo.

Para tal, calculamos todos os valores de $f_n$ usando *paralelismo quântico* sobre um estado $|x\rangle$ inicial em superposição:

$$|f_n\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} |x\rangle |f_n(x)\rangle \tag{6}$$

O estado $|f_n(x)\rangle$ resultante da aplicação função $f_n$ possui sua periodicidade, mas não está claro ainda como extraí-la. Um fato interessante é que a aplicação de $f_n$ em $|x\rangle$ torna-o *emaranhado* a $|f_n(x)\rangle$. Portanto, ao medirmos $|f_n(x)\rangle$ teremos um valor $y_0$ e o estado $|x\rangle$ tornará-se uma superposição de todos valores $x$ tais que $f_n(x) = y_0$. Se $x_0$ é o menor desses valores e $k$ é o menor número tal que $n \geq k.r$, podemos representar esse novo estado da entrada como:

$$|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{p=0}^{k-1} |x_0 + p.r\rangle \tag{7}$$

Se fosse realizada uma medição em $|\psi\rangle$ não conseguiríamos extrair $r$, pois a presença do $x_0$ torna o resultado inútil. É nesse momento que a Transformada Discreta de Fourier (**DFT**) possui utilidade. A DFT consegue representar uma função de domínio finito em uma base periódica e insensível a deslocamentos. Como essa transformação é unitária, podemos aplicá-la a um estado quântico e se fizermos isso a $|\psi\rangle$ temos:

$$\mathcal{F}|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{x_0 j}{r}} |j\frac{n}{r}\rangle \tag{8}$$

Note agora, que $x_0$ não aparece mais no estado quântico, portanto, ao medirmos $\mathcal{F}|\psi\rangle$ obteremos $c = j\frac{n}{r}$, para algum $j$ aleatório. O importante disso é que sabemos $c$ pela medição e $n$ é nosso número sendo fatorado. Como $0 \leq j \leq r-1$, há uma probabilidade de $\frac{1}{\log r}$ de que ele seja relativamente primo a $r$, e caso isso aconteça, conseguimos descobrir $r$ a partir de $c = j\frac{n}{r}$, cancelando $\frac{c}{n}$ até uma fração irredutível. Não é difícil provar que, ao realizar $O(L)$ medições de $\mathcal{F}|\psi\rangle$, é ínfima a possibilidade de não acharmos $r$.

Para garantirmos o tempo $O(L^2)$ devemos utilizar a implementação quântica da Transformada Rápida de Fourier[3].

#### 7.1.1.3 O Algoritmo.

De forma sucinta o Algoritmo de Shor utiliza os resultados da Teoria dos Números, junto a um cálculo quântico eficiente do período de uma função periódica, para fatorar números inteiros. Essa união produz um algoritmo quântico polinomial para a tarefa, como foi mostrado.

## 7.2 Comunicação Segura

Devido aos resultados do Algoritmo de Shor, a viabilidade de um computador quântico tornaria inseguro os esquemas atuais de comunicação encriptada. Em contrapartida, é

possível através da Quântica criar um canal de comunicação 100% seguro.

Existem diversas formas de implementação deste canal seguro, mas todas baseiam-se no fenômeno quântico da *não-clonabilidade*. Este fenômeno representa a impossibilidade de copiar um estado quântico superposto sem realizar um número infinito de medições. Sendo assim, se alguma pessoa espionar uma transmissão de estados quânticos estará invariavelmente alterando o estado quântico, o qual poderá ser detectado por um protocolo especial de comunicação.

A comunicação quântica segura mais conhecida é realizada através de fótons polarizados. Nela, é possível a criação de uma chave secreta compartilhada através do uso de dois tipos de medidores de polarização.

### 7.2.1 Polarização do Fóton e Bases Não-Ortogonais

A polarização de um fóton quando medida apresenta dois resultados possíveis. Já esses resultados podem ser vistos em duas bases diferentes: a base horizontal-vertical $\oplus$, com os resultados $|\updownarrow\rangle$ e $|\leftrightarrow\rangle$; e a base diagonal $\otimes$, com os resultados $|\nwarrow\rangle$ e $|\nearrow\rangle$. A existência dessas bases fornece dois padrões diferentes para representar os estados $|0\rangle$ e $|1\rangle$ de um Qubit.

Inicializando um Qubit em $|0\rangle$ ou $|1\rangle$ em alguma das bases citadas, temos um estado superposto em relação à outra. Isso porque, essas bases são não-ortogonais. Por exemplo, caso enviemos um $|0\rangle$ na base $\oplus$ para alguém e a outra pessoa utilizar a base $\otimes$, ela terá 50% de ler ou $|0\rangle$ ou $|1\rangle$.

### 7.2.2 Protocolo de Comunicação

Duas pessoas, Alice e Bob, desejam comunicar-se de forma segura. Primeiro, elas irão definir uma chave privada compartilhada só conhecida por elas através de um canal quântico. Depois disso, irão comunicar-se de forma segura com dados encriptados.[1]

Para conseguir definir a chave compartilhada, Alice e Bob seguirão os seguintes passos:

1. Alice define um conjunto de Qubits e aleatoriamente escolhe entre as bases $\oplus$ e $\otimes$ para representar cada um deles.
2. Alice envie os fótons polarizados para Bob.
3. Bob escolhe aleatoriamente entre os medidores nas bases $\oplus$ e $\otimes$ para medir cada Qubit enviado por Alice.
4. Alice e Bob divulgam entre si as bases utilizadas.
5. Alice e Bob verificam quais Qubits tiveram as mesmas bases escolhidas e enviam suas medições nessas bases.
6. Se tudo ocorreu bem, Alice e Bob não reclamarão de divergências entre suas medições. A chave então possui o número de Qubits aceitos e se for necessário mais Qubits, reinicia-se o processo.

Uma terceira pessoa, chamada Eve, deseja saber o que Alice está enviando para Bob. Para não ser descoberta, Eve intercepta o fóton de Alice, utiliza um medidor sobre alguma das bases $\oplus$ e $\otimes$ e reenvia o fóton para Bob no valor medido. Felizmente, quando Alice e Bob verificam os Qubits onde utilizaram as mesmas bases, há uma probabilidade de $\frac{1}{4}$ do valor não ser o mesmo, expondo Eve. Isso acontece quando Eve escolhe a base errada e Bob a correta, levando o Qubit reenviado a Bob a ficar em superposição em relação a sua base.

Neste protocolo, temos uma garantia de $1 - (\frac{3}{4})^N$ de detectar um espião, onde $N$ é o número de Qubits verificados. Essa probabilidade aproxima-se rapidamente de 1, sendo ínfimamente possível não detectar o espião.

### 7.2.3 Outras implementações

A implementação através de fótons polarizados é útil para a compreensão e verificação da validade da comunicação segura, mas não é a mais eficiente. As distâncias máximas permitidas de comunicação não passam de 1 metro. Já existem outras implementações[2], beirando a comercialização, que ultrapassam a marca de kilômetros.

## 7.3 Outros algoritmos quânticos

Enquanto na Computação Quântica, as aplicações mais reais da são na área de criptografia, outros algoritmos quânticos foram propostos para demonstrar seus poderes teóricos. Um dos primeiros deles, foi o Algoritmo de Deutsch-Jozsa[5], que demonstrava como os estados *emaranhados* são determinantes para o *paralelismo quântico*. Mas o mais famoso entre os teóricos é o Algoritmo de Grover para realizar buscas sublineares em conjuntos de números não-ordenados. Esse algoritmo mostra como a Computação Quântica pode redefinir os limitantes inferiores de alguns problemas.

# 8. COMPUTADORES QUÂNTICOS REAIS

A construção de um computador clássico sofreu grandes evoluções antes de chegar ao estado atual. Nessa evolução um dos desafios foi respeitar um conjunto de restrições de estabilidade, sem as quais não seria possível construir circuitos. Entretanto, o maior desafio foi, e continua sendo, a maximização de certos objetivos, como eficiência e armazenamento.

O computador quântico possue exatamente esses desafios, porém em condições opostas. Enquanto um computador quântico já nascerá em proporções mínimas, fornecendo uma capacidade de processamento jamais visto, é muito difícil construí-lo de forma estável.

Atualmente, os esforços na construção de computadores quânticos reais estão em respeitar as seguintes condições de estabilidade:

1. Representar de forma robusta a informação quântica.
2. Realizar uma família universal de transformações unitárias (portas lógicas).
3. Preparar fielmente um estado inicial.
4. Medir o resultado da saída.

Existem muitas tecnologias que tratam essas restrições, mas duas vem apresentado resultados práticos notáveis: os ópticos e os de ressonância magnética nuclear.

**Computadores Quânticos Ópticos**

[1] Note que, um canal quântico só é necessário durante a definição da chave compartilhada. Após isso, ela será um conjunto de bits clássicos, podendo ser utilizada em um canal de comunicação clássico

[2] www.infoworld.com/article/04/09/16/HNneccryptography_1.html

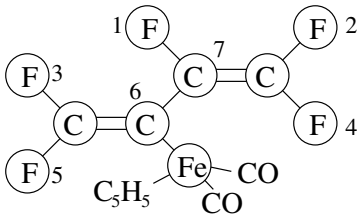


**Figura 6: A molécula utilizada para implementar um Algoritmo de Shor com 7 Qubits em um Computador Quântico de Ressonância Magnética Nuclear. Os números ao lado de alguns átomos enumeram seus respectivos Qubits.**

Nessa classe de implementações, utiliza-se fótons para representar Qubits. As transformações e medições dos estados quânticos dos fótons são feitas principalmente por aparelhos óticos. Nesse âmbito, o grande problema desse tipo de implementação está em realizar a interação entre fótons, necessária para produção de estados *emaranhados* e construção da porta NOT-Controlado. Existem duas alternativas, ou utiliza-se um meio especial (nonlinear Kerr media), atualmente não eficiente, ou cavidades eletromagnéticas em átomos. A última tem obtido melhores resultados, mas ainda está longe de viabilizar grandes interações entre fótons.

Esta dificuldade em construir as portas NOT-Controlado impede um uso amplo em Computação Quântica, mas há grandes ganhos na área de Criptografia Quântica, onde não é necessária a interação entre fótons. Além disso, fótons são fáceis de emitir e trafegam por distâncias consideráveis utilizando pouca energia, viabilizando as comunicações.

### Computadores Quânticos de Ressonância Magnética Nuclear

Atualmente, a implementação mais efetiva em Computadores Quânticos é através de Ressonância Magnética Nuclear. Nela um Qubit é representado pelo spin do núcleo atômico e, geralmente, as transformações são realizadas através de fortes campos magnéticos. O spin é medido por uma voltagem induzida pela processamento do momento magnético do núcleo.

Para implementar um registrador quântico é utilizada uma molécula, a qual é escolhida especialmente de forma que os Qubits a interagir possuam ligações químicas entre seus átomos representantes.

Sendo assim, diferentes tipos de moléculas implementam as arquiteturas necessárias para cada tipo de algoritmo quântico. Existe uma implementação do Algoritmo de Shor com 7 Qubits através da molécula da Figura 6, e do algoritmo de Grover e Deutsch-Jozsa com moléculas de Clorofórmio[2]. Invariavelmente, esses computadores perdem sua eficiência exponencialmente com o aumento de Qubits.

## 9. CONCLUSÃO

A Computação Quântica modifica os pilares da Teoria da Computação e seus ganhos são notáveis ao fornecer soluções para problemas tidos como intratáveis pela Computação Clássica, como a fatoração de inteiros.

Além disso, é possível com a Quântica criar canais de comunicação seguros que dispensam esquemas de criptografia baseados em conjecturas matemáticas.

Entretanto, a implementação real desses mecanismos ainda está em um nível muito inicial, sendo impossível dizer quando será possível utilizar desses ganhos na prática.

Existem, também, muitos outros assuntos em Quântica não tratados aqui, como: Teoria da Informação Quântica, Novas Classes de Complexidade, Correção de Códigos, Teletransporte, entre outros.

De fato, a Quântica ainda possui grande atividade no desenvolvimento de suas bases. Isso porque, mesmo sendo umas das físicas mais precisas até hoje, seus experimentos são muito controlados e facilmente perde-se a capacidade de previsão quando há uma interação com o meio. É necessário, portanto, mais conhecimento desses efeitos para viabilizar a construção de Computadores Quânticos.

## 10. REFERÊNCIAS

[1] Dirk Bouwmeester, Artur Ekert, and Anton Zeilinger. *The Physics of Quantum Information*. Springer-Verlag, Berlin Heidelberg New York, 2001.

[2] C. Macchiavello, G. M. Palma, and A. Zeilinger. *Quantum Computation and Quantum Information Theory*. World Scientific Publishing, Singapore, 1999.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[4] Peter W. Shor. Algorithms for quantum computation: Discrete log and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. Institute of Electrical and Electronic Engineers Computer Society Press, 1994.

[5] Colin P. Williams and Scott H. Clearwater. *Ultimate Zero And One*. Copernicus Springer-Verlag, New York, 2000.

[6] H. M. Wiseman. From einstein's theorem to bell's theorem: A history of quantum nonlocality. *CONTEMPORARY PHYSICS*, 47:79, 2006.