Departamento de Informática
Universidade Federal do Paraná

Uma Introdução à Computação Quântica

André Luís Vignatti
Francisco Summa Netto
Luiz Fernando Bittencourt

Fevereiro de 2004

Esse exemplar corresponde à redação
final da monografia devidamente
corrigida e defendida pelos
autores e aprovada pela banca
examinadora.

Banca examinadora:

- Prof. Dr. Jair Donadelli Júnior - UFPR (Orientador)
- Prof. Dr. André Luís Pires Guedes - UFPR
- Prof. Dr. Heraldo Maciel França Madeira - UFPR

Sumário

1 Introdução **1**
- 1.1 O desafio de Hilbert . . . 1
- 1.2 O legado de Turing . . . 1
- 1.3 Computação eficiente . . . 2
- 1.4 Vários paradigmas . . . 3
- 1.5 Computação Quântica . . . 4
- 1.6 Propósito deste documento . . . 5

2 Mecânica Quântica **7**
- 2.1 Experimento da Dupla Fenda . . . 8
- 2.2 Amplitude de Probabilidade . . . 9
- 2.3 Brackets, a notação de Dirac . . . 9
- 2.4 Espaços de Hilbert . . . 10
- 2.5 Exemplo: polarização da luz . . . 14
  - 2.5.1 Explicação . . . 15

3 O Qubit **17**
- 3.1 Distribuição quântica de chave . . . 19

4 Múltiplos qubits **25**
- 4.1 Estados justapostos . . . 25
- 4.2 Estados emaranhados . . . 27
- 4.3 Medindo Múltiplos Qubits . . . 28
- 4.4 O paradoxo EPR . . . 30
  - 4.4.1 EPR - Uma analogia . . . 31

5 Portas **33**
- 5.1 Transformações Unitárias . . . 34
- 5.2 Portas simples . . . 35
  - 5.2.1 NOT . . . 35
  - 5.2.2 Inversão de fase . . . 35

5.2.3 Hadamard-Walsh 36
5.3 Portas de múltiplos qubits 38
5.3.1 NOT-Controlado 38
5.3.2 Porta Toffoli 39
5.4 Computação reversível 39
5.5 Teorema da não-clonagem 40

6 Funções **43**
6.1 Dense Coding 45
6.2 Teletransporte 46

7 Algoritmo de Shor **51**
7.1 Introdução 51
7.2 Visão geral do algoritmo 52
7.3 Transformada quântica de Fourier 53
7.4 Passos do algoritmo de Shor 55
7.5 Expansão em frações contínuas: encontrando o período 60
7.6 Um caso especial 63

8 Algoritmo de Grover **67**
8.1 Operadores utilizados no algoritmo 68
8.1.1 Operador para rotacionar fase 68
8.1.2 Operador para criar sobreposição igual de estados . . . 69
8.1.3 Operador de inversão sobre a média 70
8.1.4 Inversão de sinal 71
8.2 Passos do algoritmo de Grover 71
8.2.1 Ilustração do algoritmo de Grover 73
8.3 Um caso especial 74

9 Complexidade Quântica **77**
9.1 Definições Iniciais 77
9.2 P $\subseteq$ QP e BPP $\subseteq$ BQP 78
9.3 NP $\subseteq$ BQP? 81
9.4 BQP $\subseteq$ NP? 81

Capítulo 1

Introdução

1.1 O desafio de Hilbert

Em 1900, o matemático David Hilbert propôs os famosos 23 desafios matemáticos para o século XX. Muitos desses problemas foram resolvidos durante o século XX, e as maiores descobertas e marcos da matemática eram atribuídos a alguém que apresentasse a solução de algum desses problemas. Hoje, o nome de Hilbert é mais bem lembrado através do conceito de *espaço de Hilbert*, que trataremos depois nesse mesmo documento. Em particular, um dos 23 problemas de Hilbert é essencial no estudo da computação. Esse problema é chamado de *Entscheidungsproblem*, uma expressão alemã que significa "problema de decisão". Por volta da época em que Hilbert enunciou o Entscheidungsproblem, muitos problemas matemáticos estavam sendo resolvidos de uma forma algorítmica. O Entscheidungsproblem desafiava justamente a criação de um procedimento genérico que resolvesse problemas matemáticos de forma algorítmica, ou, em outras palavras, era um desafio da lógica simbólica para encontrar um algoritmo genérico que decidisse se, para uma dada sentença de lógica de primeira ordem, ela é válida ou não.

1.2 O legado de Turing

Em 1936, com a idade de 24 anos, Alan M. Turing consagrou-se como um dos maiores matemáticos do seu tempo quando fez antever aos seus colegas que era possível executar operações computacionais sobre a teoria dos números por meio de uma máquina que tivesse embutidas as regras de um sistema formal. Essa máquina foi chamada de *Máquina de Turing*. Embora propriamente não existisse tal máquina, Turing enfatizou desde o início que tais mecanismos poderiam ser construídos.

A teoria foi estabelecida pela primeira vez em um artigo que tinha o título "On Computable Numbers, with an application on the Entscheidungsproblem" [36]. Ou seja, a Máquina de Turing era a resposta de Alan Turing à questão matemática de Hilbert. Nesse mesmo artigo, Turing reformulou os resultados de Kurt Gödel sobre o Teorema da Incompletude de Gödel, substituindo a linguagem aritmética formal universal pela Máquina de Turing. No mesmo artigo, Turing provou que não há solução para o Entscheidungsproblem mostrando a indecidibilidade do *Problema da Parada*, ou seja, não há algoritmo que decide se uma dada Máquina de Turing irá parar (terminar a computação). Independentemente, no mesmo ano, Alonzo Church também desenvolveu um trabalho para responder o desafio de Hilbert, no entanto o trabalho de Turing é considerado mais acessível e intuitivo.

Todos os computadores de hoje são construídos com base no modelo matemático da Máquina de Turing, por isso quaisquer limitações, dificuldades ou problemas da Máquina de Turing têm impacto direto nos computadores (hardware) que usamos hoje.

1.3 Computação eficiente

Uma série de problemas não são resolvidos por Máquinas de Turing, um exemplo é o Problema da Parada. De fato, temos que a maioria desses problemas não têm uma aplicação prática, e a impossibilidade de resolver tais problemas ainda não nos trouxe muito incômodo. Isso porque quase todas aplicações práticas são possíveis de ser computadas utilizando o modelo clássico de Máquina de Turing, e é por isso que esse modelo é bem aceito até hoje. A *tese de Church-Turing* [36, 1] estabelece que

> Todos os problemas ditos **computáveis** são problemas que são resolvidos por uma Máquina de Turing.

Chamamos de *eficientemente computáveis* os problemas cuja resposta é computada rapidamente. Mais formalmente, na teoria da complexidade computacional, os problemas eficientemente computáveis são dados pela classe P, onde P é definida como a classe dos problemas que são resolvidos na Máquina de Turing com um número de passos polinomial no tamanho da entrada. No entanto, existem vários problemas computáveis importantes para os quais não se conhece algoritmo eficiente para resolvê-los. É importante ter em mente que por não ter sido descoberto algoritmo eficiente para esses problemas, não quer dizer que tais algoritmos não existam. Ou seja, não sabemos se esses algoritmos pertecem à classe P, mas eles estão com certeza na su-

perclasse de P, que é a classe NP. Em outras palavras P $\subseteq$ NP, e a pergunta principal hoje na teoria da computação é saber se P = NP[1].

1.4 Vários paradigmas

Muitos anos se passaram desde a formulação da pergunta "P = NP?" e ainda ninguém conseguiu a resposta. Devido às limitações da Máquina de Turing, como a existência de funções não-computáveis (também ditas não-recursivas) e a existência de problemas que ainda não foram resolvidos eficientemente, pesquisadores começaram a cogitar a possibilidade de outros paradigmas de computação, visto que não havia alternativas aos modelos usuais de Máquina de Turing.

O termo *Hipercomputação* inicialmente foi apresentado por Turing num artigo de 1939 para definir funções não-recursivas que poderiam ser resolvidas por um oráculo. Esse oráculo existe somente na teoria, na prática ele não é implementável. A partir de então, a Hipercomputação foi definida como o estudo de métodos ou modelos computacionais que são concebíveis "em tese", e que são uma alternativa ao modelo usual da Máquina de Turing. Entre os modelos de Hipercomputação, estão:

- Computação com DNA;
- Computação Membrânica;
- Computação Quântica;
- Máquina de Turing Alternada;
- Máquina de Turing Paralela;
- Máquina de Turing Não-Determinística que tem uma ordem de preferência sobre seus estados finais;
- Computador "Real", ou seja, um computador capaz de operar analogicamente, ao invés de digitalmente. Esse computador seria útil, por exemplo, para computar número reais.

No estágio atual da ciência, nenhum desses dispositivos parece ser fisicamente implementável, e os hipercomputadores provavelmente serão tidos como ficção matemática. A exceção talvez seja a computação quântica, que se

[1] O "Clay Mathematics Institute" oferece U$1.000.000 a quem responder essa pergunta. A definição oficial do problema pode ser encontrada na página dessa instituição em http://www.claymath.org/Millennium_Prize_Problems/P_vs_NP.

mostrou bastante coerente em sua teoria, e mesmo que ainda não seja possível uma implementação física razoável, é bem provável que isso seja uma mera questão de tempo. Um dispositivo quântico de 7 qubits já foi construído pela IBM e conseguiu executar o algoritmo de Shor (veja Capítulo 7).

1.5 Computação Quântica

A computação quântica se mostrou bastante eficiente na resolução de alguns problemas antes tidos como intratáveis. Para compararmos o grau de eficiência da computação quântica em relação à computação clássica, temos que modificar a tese de Church-Turing de maneira que ela considere sistemas físicos. Então a forma atual (levando em consideração sistemas físicos que realizam computações) da tese de Church-Turing pode ser resumida informalmente como:

> Todas implementações físicas de dispositivos computacionais podem ser simuladas com uma sobrecarga de ordem polinomial em seu tempo de execução pela Máquina de Turing.

Atualmente, esse paradigma tem sido muito discutido, uma vez que há fortes argumentos mostrando que a tese de Church-Turing (em sua forma atual) não é aplicável em nível da física quântica, pois implementações de dispositivos quânticos provavelmente só podem ser simulados pela Máquina de Turing clássica com sobrecarga exponencial.

Os primeiros indícios dessa possibilidade ocorreram num artigo de Richard Feynman [18] que mostrava que não estava claro como simular sistemas de mecânica quântica de n partículas (n spins) em um computador sem pagar uma penalidade exponencial no tempo de simulação (mesmo usando computação probabilística). A primeira evidência formal de que computadores quânticos violam a tese modificada de Church-Turing veio uma década mais tarde, com o resultado de Bernstein e Vazirani [10], que mostrou que o tempo polinomial quântico contém o tempo polinomial probabilístico. Em 1994, Peter Shor seguiu com resultados inéditos em algoritmos quânticos, mostrando que os problemas de fatoração em primos e logaritmos discretos podem ambos serem resolvidos em tempo polinomial em um computador quântico [32]. A intratabilidade computacional desses problemas para os computadores clássicos é o padrão computacional assumido pela criptografia moderna para garantir segurança dos sistemas criptográficos. A partir do resultado de Shor, o estudo da computação quântica se intensificou.

Lov Grover [20] desenvolveu uma técnica para realizar pesquisa em uma lista não-estruturada de n itens com tempo $O(\sqrt{n})$ passos em um computador

quântico. No caso clássico, uma pesquisa em lista não-estruturada é feita em $O(n)$ passos. Contudo, a técnica de Grover fornece um aumento de velocidade polinomial, mas não exponencial como no algoritmo de Shor. Mesmo assim, é um grande avanço, que também sugere uma vantagem dos computadores quânticos sobre os computadores clássicos.

Juntos, os resultados obtidos até agora fornecem fortes evidências de que a computação quântica viola a tese atual de Church-Turing. Baseado nessas descobertas, é necessário explorar uma nova teoria da complexidade baseada na mecânica quântica.

1.6 Propósito deste documento

Esse documento tem por objetivo dar uma visão geral desse novo paradigma de computação: a computação quântica. Iremos focar nas principais diferenças entre o computador quântico e o computador clássico, apresentando uma breve introdução à mecânica quântica.

Assim como existem artigos científicos sobre computação quântica que visam os aspectos *físicos* da construção dos computadores quânticos, existem também artigos que visam os aspectos *lógicos* da construção destes. Neste documento iremos nos concentrar em aspectos lógicos da computação quântica, uma vez que, ao descrever fisicamente a construção de computadores quânticos, necessitaríamos de um estudo mais aprofundado da física quântica. Este documento é dirigido principalmente a cientistas da computação que gostariam de conhecer este assunto, por isso, estaremos focando tais aspectos lógicos da computação quântica, tentando somente explicar alguns poucos conceitos físicos necessários à compreensão. Além disso, estamos supondo que o leitor já tenha alguma familiaridade com a computação clássica, como circuitos lógicos, álgebra booleana, algoritmos, teoria da complexidade, etc. e conhecimentos de matemática, como álgebra linear, geometria analítica, números complexos, etc. No entanto, isso não exclui a possibilidade da leitura deste documento por físicos, mas advertindo a necessidade prévia de um conhecimento básico dos assuntos expostos acima. Também incluímos explicações básicas de mecânica quântica, assim os leitores com pouco ou nenhum conhecimento de física poderão acompanhar a leitura deste documento.

Finalmente, nós, os autores, temos como objetivo contribuir com a disseminação do tema deste trabalho entre os estudantes de computação, visto que ainda não foi detectada a existência de documentos de introdução à

computação quântica escritos em língua portuguesa e com texto acessível aos não-físicos.

Capítulo 2

Mecânica Quântica

Antes de apresentarmos o funcionamento da computação quântica, teremos que entender algumas noções básicas de mecânica quântica. A mecânica clássica (também chamada de mecânica newtoniana, devido a Newton ser o pioneiro em seu estudo) foi a primeira tentativa de descrever o comportamento mecânico de objetos. O principal objetivo do estudo de Newton era estabelecer as regras da física para os objetos que realizam algum tipo de movimento, por exemplo, para estabelecer com qual velocidade um corpo se movimenta se arremessado de uma altura de 10 metros, ou quantos metros um carro irá andar se impulsionado por uma força de 10.000 N.

No entanto, por meio de experimentos no início do século XX, cientistas observaram que as leis clássicas não eram aplicáveis a objetos muito pequenos. Em outras palavras, o que havia sido calculado pela mecânica clássica não refletia o comportamento de objetos extremamente pequenos. O que foi observado foi um comportamento totalmente não-intuitivo na mecânica desses objetos. A partir de então uma nova teoria que descrevesse o comportamento de objetos microscópicos teve de ser construída. Obviamente deve haver uma linha-limite no tamanho dos objetos para que o comportamento desses se enquadre na mecânica clássica ou na mecânica quântica. Nessa linha-limite estão objetos que são aproximadamente 100 vezes maiores que o tamanho de um átomo de hidrogênio. Objetos menores que isso têm seu comportamento descrito na mecânica quântica, enquanto que objetos maiores são tratados pela mecânica newtoniana.

Matematicamente falando, a mecânica quântica é uma teoria, pois é regida por um conjunto de axiomas (princípios). As conseqüências desses axiomas descrevem o comportamento dos sistemas da mecânica quântica.

Iniciaremos com um exemplo, para demonstrar que o comportamento intuitivo clássico não é aplicável à mecânica quântica.

2.1 Experimento da Dupla Fenda

Considere uma divisória com duas fendas estreitas e paralelas. De um lado dessa divisória coloca-se uma fonte de luz forte (pode-se utilizar uma caneta laser, geralmente usada para apontar textos). A maior parte da luz atingirá a divisória, mas uma pequena parcela atravessará as fendas. Suponha agora que coloque-se uma tela do outro lado da divisória. Se somente uma fenda está aberta, a intensidade da luz na tela atinge seu máximo na posição diretamente na linha da fenda. Quando ambas as fendas estão abertas, o que é visto na tela não é somente duas posições as quais a luz incide, e sim um padrão característico de franjas claras e escuras. Esse efeito é causado pela interferência da luz vinda das duas fendas. Surpreendentemente, a interferência continua mesmo quando a fonte de luz emite somente um fóton, ou seja, o mesmo padrão de franjas aparece. Cada fóton parece interferir em si mesmo.

Diversos conceitos físicos estão envolvidos na explicação desse fenômeno. Mas nosso principal objetivo com esse exemplo é traduzir tal fenômeno para o "vocabulário" da mecânica quântica.

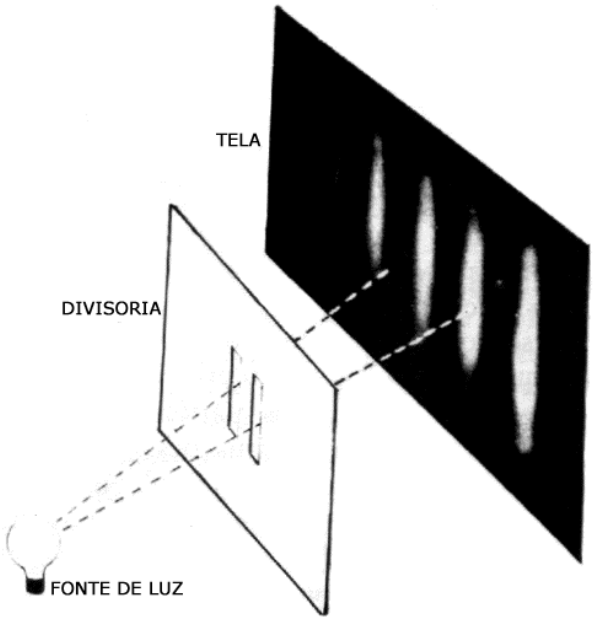


Figura 2.1.1: Experimento da dupla fenda.

2.2 Amplitude de Probabilidade

O experimento da fenda dupla é um exemplo clássico no estudo da mecânica quântica. O objetivo deste exemplo não é explicar o porquê do comportamento estranho (para explicar isso, teríamos que aprofundar o estudo da física, o que não é o propósito deste documento), mas estabeler as regras que causam esse tipo de comportamento. Através deste capítulo, vamos enunciar os princípios da mecânica quântica.

Definição 2.2.1. *Dado um experimento, um* evento *é o conjunto de estados iniciais e finais.*

Por exemplo, no experimento da dupla fenda, *"um fóton sai da origem s (feixe de luz) e chega na parede na posição x"* é um evento. O objetivo da mecânica quântica é prever se um dado evento pode acontecer ou não, baseado em seus estados iniciais e finais e nas transformações que acontecem no estado quântico entre o estado inicial e final. O primeiro princípio define a probabilidade de um dado evento ocorrer.

Primeiro Princípio. *A probabilidade*[1] *p de um evento ocorrer é dada pela norma quadrada*[2] *de um número complexo α (onde α é chamado* amplitude de probabilidade *ou simplesmente* amplitude*), ou seja:*

$$p = ||\alpha||^2.$$

A amplitude de probabilidade α é um evento que será denotado por:

$$\alpha = \langle \text{ estado final } | \text{ estado inicial } \rangle.$$

Ou, no exemplo do experimento da fenda dupla:

$$\langle \text{ partícula chegou na posição } x \mid \text{ partícula sai da origem } s \rangle.$$

2.3 Brackets, a notação de Dirac

A notação que representa a amplitude de probabilidade α apresentada acima é chamada de *notação de Dirac* (que a princípio foi inventada para a probabilidade condicional). Em mecânica quântica, essa notação é utilizada devido à

[1] Na mecânica quântica, o conceito de probabilidade é o mesmo conceito utilizado na teoria da probabilidade.

[2] A norma quadrada da amplitude de probabilidade $||w||^2$ é definida como a^2+b^2, sendo $w = a + ib$. Algumas vezes nesse documento iremos denotar $||w||^2$ por w^2 para simplificar a notação e tornar fórmulas mais legíveis.

sua praticidade em representar as transformações e estados quânticos, como veremos adiante. O simbolo $\langle\psi|$ é chamado de *bra*, o símbolo $|\psi\rangle$ é chamado de *ket*. A notação $\langle\phi|\psi\rangle$ é então chamada de *bracket*.

Tomando o experimento da fenda dupla, $\langle x|s\rangle$ denota a amplitude da partícula de luz (fóton) sair de s e chegar em x. Continuando com o mesmo exemplo, note que poderíamos dividir esse evento em dois sub-eventos sequenciais. O primeiro evento seria a ação da partícula sair da origem chegando à divisória, e no segundo evento a partícula sairia da divisória chegando à parede. A amplitude de probabilidade poderia ser representada como:

$$\langle x|\text{divisória}\rangle\langle\text{divisória}|s\rangle. \tag{2.3.1}$$

A amplitude de probabilidade de um fóton emitido da origem passar pela fenda número 0 ou 1, depois chegar à posição x da parede é:

$$\langle x|s\rangle = \langle x|0\rangle\langle 0|s\rangle + \langle x|1\rangle\langle 1|s\rangle. \tag{2.3.2}$$

Assim sendo, podemos agora definir o segundo e terceiro princípios da mecânica quântica, que falam sobre o produto e soma de amplitudes, respectivamente.

Segundo Princípio. *Se um evento pode ser separado em outros dois sub-eventos sequenciais, a amplitude do evento é o produto das amplitudes de cada um dos sub-eventos.*

Terceiro Princípio. *Se um evento pode ocorrer de várias maneiras diferentes, então a amplitude do evento é a soma das amplitudes de cada uma das maneiras separadamente.*

Podemos observar que a notação de Dirac, utilizada acima, é consistente, ou seja, a notação consegue descrever todas as possibilidades de eventos que podem realmente ocorrer no estado quântico. Por exemplo, analisando pela notação, é impossível um fóton sair da origem s, entrar na fenda 0, sair da fenda 1 e chegar ao destino x. Isso porque, pela notação, temos somente duas possibilidades: $\langle x|0\rangle\langle 0|s\rangle$ (fóton entra pela fenda 0 e sai pela fenda 0) ou $\langle x|1\rangle\langle 1|s\rangle$ (fóton entra pela fenda 1 e sai pela fenda 1).

2.4 Espaços de Hilbert

Até agora estamos tratando os eventos s e x como o *evento de origem e destino*, respectivamente, mas ainda não foi definido um modelo matemático para representar tais eventos. Todos os eventos que acontecem durante a

evolução dos estados em um sistema quântico são modelados matematicamente no espaço de Hilbert das funções de ondas. No entanto, para a compreensão da computação quântica, é necessário somente o conhecimento de sistemas quânticos finitos. Em outras palavras, não necessitaremos modelar sistemas quânticos no espaço de Hilbert das funções de ondas (que é usado para modelagens de sistemas infinitos). Consideraremos somente os espaços de Hilbert que são *espaços vetoriais complexos de dimensão finita*, assim temos a vantagem de não precisarmos nos preocupar com funções de onda.

Um *espaço vetorial complexo* é um espaço vetorial cujos vetores possuem coordenadas (e conseqüentemente comprimentos), descritos por números complexos.

Da definição de espaço vetorial, temos que todo espaço vetorial é gerado por uma *base*. A base do espaço vetorial, por sua vez, é formada por *vetores da base* ou simplesmente *vetores-base*. Em um espaço vetorial com duas dimensões, precisamos de uma base formada por pelo menos 2 vetores-bases, que possibilitam descrever qualquer vetor nesse espaço. Em um espaço vetorial com três dimensões, precisamos de uma base com ao menos 3 vetores-bases, e assim por diante. Isso nos leva ao quarto princípio da mecânica quântica.

Quarto Princípio. *Qualquer evento pode ser descrito em termos de um conjunto de estados-base quando fornecemos as transições de origem e destino desses estados bases.*

Como veremos adiante, os estados-base são na verdade descritos como vetores-base. Além disso, o termo *transição* utilizada na definição do Quarto Princípio será descrita quando falarmos de transformações unitárias e portas quânticas, por hora basta saber que existem transições (transformações) entre estados.

Para algum dado evento podemos considerar uma base formada por infinitos vetores-base, no entanto isso nem sempre é prático visto que queremos definir o evento sobre uma base formada por um conjunto finito vetores-base. No experimento da fenda dupla, temos uma base formada aparentemente por somente dois vetores-base (B=$\{0,1\}$, representando as fendas 0 e 1 respectivamente). Poderíamos pensar em considerar mais vetores de base para esse experimento, no entanto nenhum vetor-base adicional seria de utilidade para descrever o evento, isso porque, ao considerar as fendas 0 e 1 como vetores da base, já é suficiente para descrever todos os possíveis eventos do sistema.

Além disso, a notação de Dirac para espaços vetoriais adquire um significado adicional. Um *ket* como $|x\rangle$ denota vetores em *coluna* e são geralmente

usados para descrever estados quânticos. O *bra* $\langle x|$ denota a conjugada[3] transposta de $|x\rangle$, e é denotado por um vetor em *linha*.

Por exemplo, no experimento da dupla fenda, poderíamos definir[4] as bases 0 e 1 como

$$\text{base } 0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle,$$

$$\text{base } 1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

De acordo com a notação de Dirac para espaços vetoriais, $\langle\phi|\psi\rangle$ agora denota o *produto interno* entre esses dois vetores. Por exemplo, sejam $|0\rangle$ e $|1\rangle$ duas bases ortonormais.[5] Como $|0\rangle$ é um vetor unitário, então $\langle 0|0\rangle = 1$ e como $|0\rangle$ e $|1\rangle$ são ortonormais, então $\langle 0|1\rangle = 0$. A notação $|\phi\rangle\langle\psi|$ significa o *produto vetorial* (produto externo) dos dois vetores. Podemos também expressar $|\phi\rangle\langle\psi|$ em forma de matrizes. Por exemplo, $|0\rangle\langle 1|$ poderia ser escrito em sua forma matricial, onde $|0\rangle = (1,0)^T$, $\langle 0| = (1,0)$, $|1\rangle = (0,1)^T$, $\langle 1| = (0,1)$, então:

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Como visto acima, um *ket* $|x\rangle$ é uma maneira útil e concisa para descrever as bases (e estados como um todo) de um espaço vetorial.

Note que ainda não foi explicada qual a ligação entre o significado definido na equação (2.3.1) com a representação de brackets em vetores apresentada acima. Vamos esclarecer isso agora. Seja $B = \{b_1, b_2, \ldots, b_n\}$ a base de um sistema (onde os b_i são os vetores da base). Seja Y o estado inicial do evento $\langle X|Y\rangle$. Uma vez que estamos somente interessados no estado inicial e nas trasformações que levarão esse estado inicial a algum estado final previamente desconhecido, então podemos suprimir $\langle X|$ do evento (pois a princípio o estado X é desconhecido), ficando somente com $|Y\rangle$. Supondo que há dois vetores-base na base do sistema quântico, o vetor $|Y\rangle = (y_0, y_1)^T$ é expresso como combinação linear destes dois vetores-base da seguinte maneira:

$$|Y\rangle = y_0|0\rangle + y_1|1\rangle.$$

[3] O complexo conjugado de um número complexo $z = a+bi$ é definido como $z^* = a-bi$. A matriz conjugada da matriz A é a matriz obtida substituindo cada elemento $a_{j,k} \in A$ pelo seu complexo conjugado $a^*_{j,k}$.

[4] Não importa se as bases 0 e 1 forem definidas como $(1,0)^T$ e $(0,1)^T$ respectivamente, ou como $(0,1)^T$ e $(1,0)^T$ respectivamente, o que importa é que a representação permaneça consistente.

[5] Base ortonormal é uma base ortogonal onde os vetores da base são unitários.

Onde, por definição $b_0 = |0\rangle = (1,0)^T$ e $b_1 = |1\rangle = (0,1)^T$. Podemos também representar Y em forma de somatório:

$$|Y\rangle = \sum_{i=0}^{1} y_i |b_i\rangle.$$

Genericamente, Y poderia ser combinação linear de n vetores-base. Sua representação então seria:

$$|Y\rangle = \sum_{i=0}^{n} y_i |b_i\rangle.$$

Note que $y_i = \langle b_i|Y\rangle$, pois y_i é a projeção do vetor Y no vetor-base b_i. Assim, podemos reescrever o somatório da seguinte forma:

$$|Y\rangle = \sum_{i=0}^{n} \langle b_i|Y\rangle |b_i\rangle.$$

O resultado do produto interno $\langle b_i|Y\rangle$ é um número complexo que será denotado a partir de agora como α_i, onde $\alpha_i = \langle b_i|Y\rangle$ é a amplitude do sistema com relação a cada estado-base b_i. Isso simplifica a notação:

$$|Y\rangle = \sum_{i=0}^{n} \alpha_i |b_i\rangle. \tag{2.4.3}$$

No vocabulário da mecânica quântica, dizemos que o estado $|\psi\rangle$ *colapsa* em b_i quando é realizada uma *medição* em $|\psi\rangle$, e esse é projetado no vetor-base b_i. Não vamos nos preocupar por enquanto com o significado de medição, que será explicado com mais detalhes posteriormente.

O Primeiro Princípio nos diz que a probabilidade de um dado evento $\langle\phi|\psi\rangle$ ocorrer é dada pela norma quadrada do evento. Por exemplo, em $|Y\rangle = \sum_{i=0}^{1} \alpha_i |b_i\rangle$, o α_i por si só representa a amplitude do evento do estado Y colapsar no estado-base b_i (pois $\alpha_i = \langle b_i|Y\rangle$). Então $||\alpha_i||^2$ é a probabilidade de Y colapsar em b_i. A soma de todas as n probabilidades resulta em 1, como conhecemos da teoria da probabilidade. Assim, podemos enunciar o quinto princípio:

Quinto Princípio. *Para qualquer conjunto de estados-base B e um estado inicial Y,*

$$\sum_{i \in B} ||\langle i|Y\rangle||^2 = 1.$$

Ou seja, a soma das probabilidades de qualquer sistema quântico é 1.

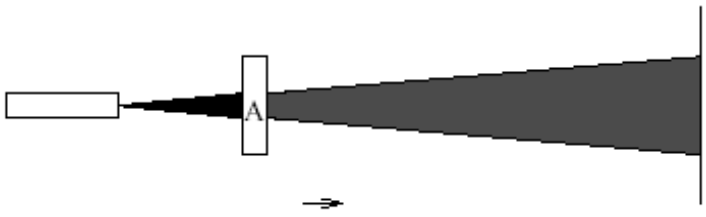
Olhando novamente a equação (2.4.3), naturalmente pensamos que, como Y é um estado, então ele deve estar colapsado em algum de seus vetores-base. Ou seja, intuitivamente achamos que $Y = \alpha_0|b_0\rangle$ ou $Y = \alpha_1|b_1\rangle$ ou $Y = \alpha_i|b_i\rangle$. Entretando, essa maneira intuitiva de pensar está errada. O estado Y representa os n estados *ao mesmo tempo*(!), contrariando qualquer noção intuitiva da mecânica clássica. Dizemos então que Y está num estado de *sobreposição*, ou seja, vários estados estão sobrepostos simultaneamente. Se queremos medir os valores sobrepostos de Y para saber em qual estado Y está, então Y colapsa em algumas de suas bases b_i com probabilidade $||\alpha_i||^2$ (também denotado por α_i^2 para simplificação da notação).

2.5 Exemplo: polarização da luz

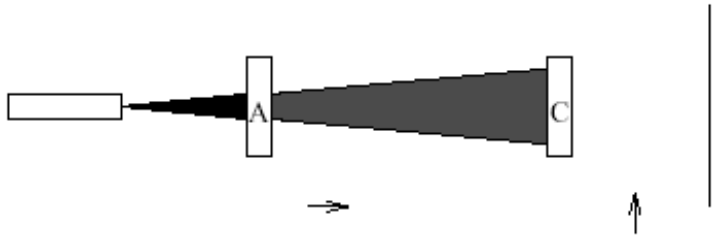
Antes de finalizarmos nossa breve introdução da mecânica quântica, apresentaremos um exemplo para demonstrar na prática o uso dos conceitos, para então continuarmos o estudo da computação quântica. O exemplo é seguido de uma explicação que utilizará os conceitos de mecânica quântica vistos até agora. Para a realização do experimento, necessitamos de uma fonte de luz forte (pode-se utilizar uma caneta laser, geralmente usada para apontar textos), três filtros de polarização (os quais podem ser conseguidos em lojas de câmeras fotográficas).

O feixe de luz é projetado em uma parede. Os filtros A, B, C de polarização devem ser de polarização horizontal, 45°, e vertical, respectivamente, e devem ser colocados entre o feixe de luz e a parede.

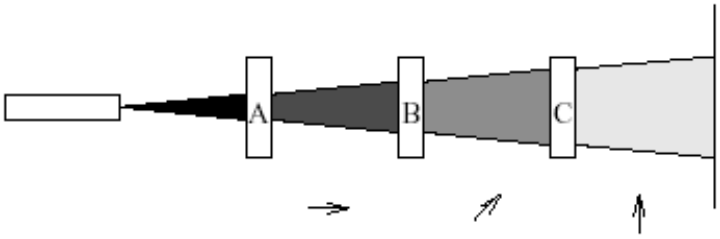
Primeiro, colocamos somente o filtro A (de polarização horizontal) em frente à luz. Como resultado, observamos que, a luz, ao passar pelo filtro A perde a intensidade em aproximadamente 50%.



Agora, vamos colocar agora o filtro C entre o filtro A e a parede. A luz do feixe foi totalmente bloqueada pelos filtros, e não há luz incidente na parede.



O filtro B é então colocado entre os filtros A e C. Observa-se agora que há luz incidente na parede, mas com uma intensidade muito baixa.



Mesmo assim, esse resultado é curioso. Quando havia somente os filtros A e C, a luz não passava. Ao adicionar o filtro B entre A e C, a luz agora incide na parede. Mas intuitivamente, ao adicionar mais um filtro, isso dificultaria ainda mais a passagem de luz. A mecânica quântica tem uma explicação para esse fenômeno.

A polarização da luz, assim como a dupla fenda, é um dos poucos experimentos da mecânica quântica que pode ser visto a olho nu, sem o auxílio de equipamentos. Por essa razão, escolhemos esse experimento como exemplo. Uma vez que estamos acostumados com os princípios da mecânica clássica (newtoniana), a polarização do fóton nos revela resultados não intuitivos. A seguir, uma vamos explicar esse comportamento, utilizando alguns conceitos básicos de mecânica quântica.

2.5.1 Explicação

Seja $\langle d|s\rangle$ o evento que descreve a saída dos fótons da origem da luz s chegando à parede d. Ao colocarmos o filtro A entre s e d, temos que:

$$\langle d|s\rangle = \langle d|A\rangle\langle A|s\rangle.$$

Assumindo que os fótons saem de s com polarização aleatória, e como o filtro A mede os fótons com relação à base horizontal (que iremos representar por $\leftrightarrow$), então somente 50% dos fotóns passarão pelo filtro A. Então, $\langle A|s\rangle^2 = 1$, ou seja, a probabilidade dos fótons que saem da origem s atingirem A é de

100%. No entanto, $\langle d|A\rangle^2 = 1/2$, pois o filtro A deixa passar somente os fótons que forem medidos com tendo polarização $\leftrightarrow$. Assim:

$$\langle d|s\rangle^2 = \langle d|A\rangle^2\langle A|s\rangle^2 = (1/2)1 = 1/2.$$

Como todos os fótons que estão entre A e d estão no estado $|\leftrightarrow\rangle$, ao colocar o filtro C entre A e d, nenhum fóton irá passar, pois C mede com relação à base vertical ($\updownarrow$). No entanto, ao colocarmos o filtro B entre A e C, B mede com relação à base de $45°(\nearrow)$ e deixa passar alguns fótons para C. Isso porque a base $|\nearrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$. Portanto, dos fótons que passaram por A, 50% serão medidos por B como $\leftrightarrow$, e 50% serão medidos como $\updownarrow$. Então a probabilidade do sistema é representada como:

$$\langle d|s\rangle^2 = \langle d|C\rangle^2\langle C|B\rangle^2\langle B|A\rangle^2\langle A|s\rangle^2 = (1/2)(1/2)(1/2)1 = 1/8.$$

Capítulo 3

O Qubit

Os cinco princípios enunciados anteriormente estão descritos de uma forma genérica e estão presentes em qualquer sistema quântico. Agora, vamos focar nossa atenção a princípios mais específicos da mecânica quântica que servem para criar o modelo computacional quântico.

A estrutura básica de informação na computação clássica é o *bit*, a estrutura análoga na computação quântica é o bit quântico, que é chamado de *qubit*. Vamos começar definindo formalmente um qubit.

Definição 3.0.1. *Um* ***qubit*** *é um estado quântico* $|\varphi\rangle$ *da forma*

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

onde $\alpha, \beta \in \mathbb{C}$ *e* $\alpha^2 + \beta^2 = 1$.

Em outras palavras, o qubit $|\varphi\rangle$ pode colapsar na base $|0\rangle$ com probabilidade α^2, ou na base $|1\rangle$ com probabilidade β^2.

Na definição acima, nada é dito sobre o meio físico em que as bases do qubit são construidas. As bases $|0\rangle$ e $|1\rangle$ podem ser fisicamente codificadas como spin-up e spin-down de uma partícula, direção vertical e horizontal de polarização, etc... Felizmente, para que possamos entender o funcionamento de computadores quânticos, não se faz necessária a abordagem dos aspectos físicos envolvidos na criação destes. Ou seja, a nossa definição de qubit (3.0.1) é uma abstração da implementação física, mas nem por isso deixa de ser menos significativa ou dificulta o entendimento dos conceitos da computação quântica.

A principal diferença entre o bit clássico e o bit quântico é que o bit clássico pode estar somente com um valor armazenado num determinado instante, esse valor é 0 ou 1. O bit quântico (qubit) está numa sobreposição

de $0's$ e $1's$ num determinado instante, ou seja, 0 e 1 estão armazenados ao mesmo tempo. Realizar uma medição de um sistema quântico é um problema central na teoria quântica, e muitos estudos foram e continuam sendo feitos nessa área. O problema é que, num computador clássico, é possível a princípio saber sobre o estado de qualquer bit em memória, sem alterar o sistema. Num computador quântico, a situação é diferente. Qubits podem estar em estados sobrepostos, ou até mesmo "emaranhados" (como veremos depois), e o simples ato de medir um estado quântico altera seu estado.

Um qubit pode ser geometricamente visualizado em três dimensões, como na Figura 3.0.1. Essa representação geométrica é chamada de *esfera de Bloch*. Devido à restrição de normalização (i.e, a norma do vetor no espaço de Hilbert deve ser igual a 1), nós podemos expressar genericamente o estado de um qubit como $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\text{sen}\frac{\theta}{2}|1\rangle$, onde os ângulos θ e ϕ definem um ponto na esfera[1]. Como veremos depois, todas as transformações que ocorrem num qubit são na verdade rotações do vetor $|\psi\rangle$ na esfera de Bloch.

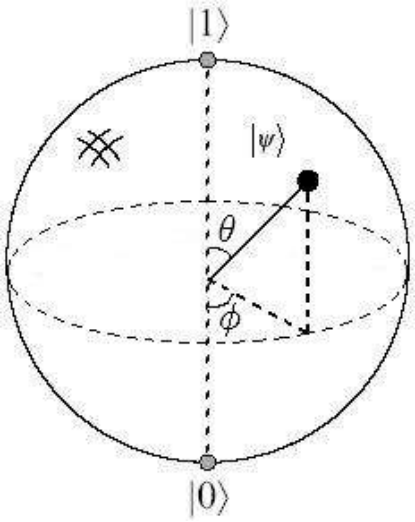


Figura 3.0.1: Esfera de Bloch: representação 3D do qubit.

Fazer uma medição em um qubit num dado estado irá retornar 0 com probabilidade α^2 e 1 com probabilidade β^2 e, mais importante que isso, o estado do qubit depois da medição será $|0\rangle$ ou $|1\rangle$ (somente uma das duas

[1]Um vetor $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ pode ser representado como $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\text{sen}\frac{\theta}{2}|1\rangle$ devido à polarização elíptica, restrição de normalização e coordenadas esféricas. Não iremos nos aprofundar nessa explicação, para os propósitos desse documento basta saber a forma genérica do qubit do modo como foi enunciado.

possibilidades), e *nunca* será outra sobreposição do tipo $\alpha|0\rangle + \beta|1\rangle$. As regras da mecânica quântica são bem rígidas quanto a isso, ou seja, é impossível realizar medição sem que o vetor-estado colapse em alguma base. As observações acima traduzem o sexto princípio da mecânica quântica.

Sexto Princípio. *Seja $|\varphi\rangle$ um vetor-estado de um espaço de Hilbert H. Seja $B = b_0, b_1, \ldots, b_k$ o conjunto das bases de H.*

$$|\varphi\rangle = \sum_{i=0}^{k} \alpha_i |b_i\rangle.$$

*Ao **medir** (observar) o estado $|\varphi\rangle$:*

1. *Somente uma das bases b_i será selecionada, com probabilidade α_i^2.*
2. *O estado $|\varphi\rangle$ irá colapsar na base b_i selecionada.*
3. *A única informação obtida pela medição é o valor b_i selecionado. Todas outras informações (que antes da medição estavam sobrepostas) serão perdidas.*

Para não perdermos o estado atual de um qubit quando o medimos, uma boa idéia seria clonar os estados. No entanto, como veremos adiante, a clonagem de estados quânticos é impossível de ser realizada.

3.1 Distribuição quântica de chave

Seqüências de qubits podem ser usadas para transmitir chaves privadas em meios não seguros. Classicamente, técnicas de criptografia com chave pública (por exemplo, o RSA [2]) são usadas para fazer distribuição de chaves. O objetivo desta seção é mostrar como os princípios da mecânica quântica podem ser usados para construir sistemas de comunicação criptográfica, fazendo com que o sistema detecte se há alguém tentando escutar os dados, garantindo que não há pessoas espionando a comunicação.

Considere a seguinte situação: Alice e Bob querem trocar uma chave secreta para então eles poderem comunicar-se com segurança. Eles estão conectados por um canal aberto bidirecional e um canal quântico unidirecional. As informações de ambos os canais estão sendo observadas por Eve, que quer espionar a transmissão e conseguir a chave secreta que descriptografa os textos enviados por Alice e Bob. As situação está ilustrada na Figura 3.1.2.

Nesse exemplo, usaremos os estados polarizados do fóton para transmitir as informações. O canal quântico permite que Alice envie fótons para Bob,

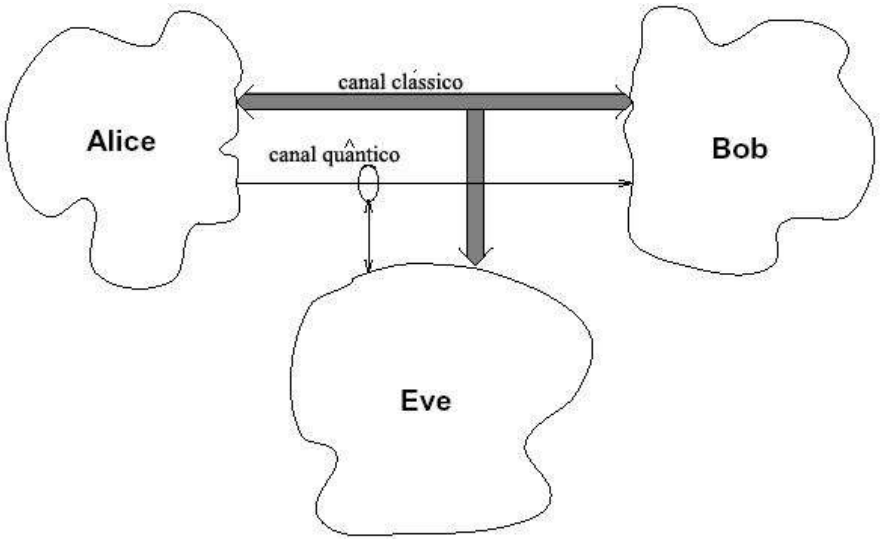


Figura 3.1.2: Esquema da distribuição de chave

que irá medir o estado quântico desses fótons. Eve, a espiã, pode capturar esses fótons e medí-los antes deles chegarem em Bob. Mas para tentar passar despercebida, ela reenvia os fótons a Bob.

O processo de estabelecer uma chave secreta começa com Alice enviando uma sequência de bits para Bob. Cada bit a ser enviado é codificado em um estado quântico do fóton. Se Alice decide usar a base Vertical-Horizontal (VH) (que denotaremos por $\boxplus$) para codificar um bit, então Alice estará usando o seguinte *alfabeto quântico*:

$$\begin{cases} \text{“1”} & = & |\updownarrow\rangle\,, \\ \text{“0”} & = & |\leftrightarrow\rangle\,. \end{cases}$$

Em outras palavras, se Alice usar esse alfabeto quântico para codificar os bits em estados quânticos que passarão pelo canal quântico unidirecional, ela irá transmitir um “1” para Bob simplesmente enviando um fóton no estado de polarização $|\updownarrow\rangle$, e transmitirá um “0” enviando um fóton no estado de polarização $|\leftrightarrow\rangle$.

Por outro lado, se Alice decide usar a base oblíqua (denotada por $\boxtimes$), então ela irá usar o seguinte *alfabeto quântico*:

$$\begin{cases} \text{“1”} & = & |\nearrow\rangle\,, \\ \text{“0”} & = & |\nwarrow\rangle\,. \end{cases}$$

Enviar um "1" significa enviar um fóton no estado de polarização $|\nearrow\rangle$, e enviar um "0" significa enviar um fóton no estado de polarização $|\nwarrow\rangle$.

Vamos agora definir como funciona o protocolo para distribuição de chave.

Protocolo - Estágio 1: Comunicação sobre o canal quântico

Passo 1. Alice gera uma sequência aleatória de 0's e 1's. Essa sequência será usada para construir a chave secreta compatilhada somente com Bob.

Passo 2. Para cada bit da sequência aleatória, Alice escolhe aleatoriamente um dos dois alfabetos quânticos. Ela então transmite o fóton polarizado de acordo com o alfabeto escolhido.

Passo 3. Cada vez que Bob recebe um fóton enviado por Alice, como ele não sabe qual alfabeto quântico Alice escolheu, então ele seleciona aleatoriamente um dos dois alfabetos para fazer a medição do fóton de acordo com a base do alfabeto escolhido. Metade das vezes, Bob terá sorte de ter escolhido o mesmo alfabeto que Alice escolheu. Nesse caso, o bit resultante de sua medição será igual ao bit enviado por Alice. No entanto, na outra metade das vezes, Bob não terá sorte e não escolherá o alfabeto que Alice usou. Nesse caso, o bit resultante da medição de Bob irá ser igual ao bit enviado por Alice somente 50% das vezes. Depois de medir todos os fótons enviados, Bob também tem uma sequência binária.

Alice e Bob agora começam a comunicação sobre o canal bidirecional aberto usando o estágio 2 do protocolo:

Protocolo - Estágio 2: Comunicação sobre canal aberto

Fase 1. *Extração da chave inicial.*

Passo 1. Através do canal aberto, Bob envia a Alice quais alfabetos quânticos ele usou para cada uma das medições dos fótons enviados por ela.

Passo 2. Em resposta, Alice envia a Bob no canal aberto quais das medições foram realizadas com o alfabeto correto.

Passo 3. Alice e Bob apagam todos os bits que obtiveram alfabetos quânticos incompatíveis. Os bits que restaram (que tiveram o mesmo alfabeto) formam a *chave inicial*. Se Eve não espionou, então a chave resultante de Alice será igual a chave inicial resultante de Bob. Se Eve espionou, então as chaves iniciais de Alice e Bob serão diferentes.

Fase 2. *Estimar o erro.*

Passo 1. No canal aberto, Alice e Bob comparam pequenas partes das sua chaves iniciais para estimar a taxa de erro R, e então deletam os bits que foram revelados no canal aberto da chave inicial, formando a *possível chave definitiva*. Se durante a troca de informações no canal público, Alice e Bob não acharem discrepâncias nos bits (i.e, $R = 0$), então eles sabem que Eve não estava espionando e a possível chave definitiva se torna a *chave final*. Se eles descobrirem pelo menos um erro durante a troca de informações no canal público (i.e, $R > 0$), então eles sabem que Eve estava espionando. Nesse caso, eles descartam suas possíveis chaves definitivas e devem começar o processo (protocolo) novamente.

As tabelas abaixo exemplificam o funcionamento do protocolo. Lembrando que a base vertical-horizintal é denotada por ⊞ e a base oblíqua é denotada por ⊠. Nessa primeira tabela, a comunicação é feita sem a intervenção de Eve:

Alice	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
	↕	↖	↖	↗	↕	↖	↔	↗	↔	↗
	1	0	0	1	1	0	0	1	0	1
	|		|				|		|
	*		*					*		*
	|		|				|		|
Bob	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
	1	0	1	1	1	0	0	0	0	0
					⇕					
Chave ⇒		0		1	1	0	0		0	

Se Eve conseguir interceptar cada qubit recebido de Alice e medi-lo, e então, reenviar o qubit a Bob com o estado que ela (Eve) mediu, então Eve estará introduzindo uma taxa de erro de 25% na chave inicial de Bob. Por isso, no final as chaves de Alice e Bob não são iguais. Na tabela abaixo, exemplificamos a comunicação com a intervenção de Eve:

Alice	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
	↕	↖	↖	↗	↕	↖	↔	↗	↔	↗
	1	0	0	1	1	0	0	1	0	1

Eve	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞
	1	0	1	1	1	1	0	1	0	0

Bob	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
	1	0	1	1	1	1	1	0	0	0
	∗	0	∗	1	1	1	1	∗	0	∗
						E	E			

Capítulo 4

Múltiplos qubits

Já definimos o qubit, agora trataremos sobre vários qubits num mesmo sistema quântico. Múltiplos qubits reservam outras propriedades da mecânica quântica, que são essenciais para o desenvolvimento dos algoritmos quânticos que serão vistos posteriormente. Chamaremos um conjunto de qubits de *registrador quântico*, ou simplesmente *registrador*. Assim como no caso clássico, os registradores quânticos podem ser usados para guardar informações mais complexas, que requerem maior espaço.

4.1 Estados justapostos

Sejam Q_1 e Q_2 sistemas quânticos. Imagine que esses dois sistemas foram configurados separadamente nos estados $|\psi_1\rangle$ e $|\psi_2\rangle$ respectivamente, e depois foram unidos sem que houvesse interação entre eles. Devido aos sistemas Q_1 e Q_2 terem sidos separadamente configurados sem que houvesse interação, seus estados $|\psi_1\rangle$ e $|\psi_2\rangle$ estão em distintos espaços de Hilbert H_1 e H_2, respectivamente. Portanto, qualquer alteração em algum dos estados não irá afetar a configuração do outro estado.

O sistema quântico global Q, que consiste dos sistemas quânticos Q_1 e Q_2, como descritos acima, é chamado de *justaposição* dos sistemas quânticos Q_1 e Q_2.

O estado $|\psi\rangle$ de Q pode ser representado como:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_1\rangle \in H_1 \otimes H_2.$$

Onde $\otimes$ representa o *produto tensorial*. Em geral, os estados quânticos são descritos através do produto tensorial, e estados não-quânticos (i.e., da computação clássica) são descritos através do produto cartesiano. Compreender mais a fundo as diferenças entre os produtos cartesiano e tensorial é fundamental para o entendimento da computação quântica.

Sejam V e W dois espaços vetoriais complexos de duas dimensões, com bases $\{v_1, v_2\}$ e $\{w_1, w_2\}$ respectivamente. O produto cartesiano desses dois espaços tem como base a união das bases de V e W, $\{v_1, v_2, w_1, w_2\}$. Note que a ordem das bases foi escolhida arbitrariamente e que a dimensão do espaço cresce linearmente, pois $\dim(V \times W) = \dim(V) + \dim(W)$. Por outro lado, o produto tensorial de V e W tem como base $\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\}$. Novamente a escolha da ordem das bases pode ser feita arbitrariamente. No entanto, a dimensão do novo espaço agora é dada por $\dim(V \otimes W) = \dim(V) \times \dim(W)$. Se temos três qubits, todos usando a base $\{|0\rangle, |1\rangle\}$, e queremos colocá-los juntos no mesmo espaço de Hilbert, então o novo espaço terá como base $\{|0\rangle \otimes |0\rangle \otimes |0\rangle; |0\rangle \otimes |0\rangle \otimes |1\rangle; |0\rangle \otimes |1\rangle \otimes |0\rangle; |0\rangle \otimes |1\rangle \otimes |1\rangle; |1\rangle \otimes |0\rangle \otimes |0\rangle; |1\rangle \otimes |0\rangle \otimes |1\rangle; |1\rangle \otimes |1\rangle \otimes |0\rangle; |1\rangle \otimes |1\rangle \otimes |1\rangle\}$, que pode ser escrito de uma forma mais compacta como $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

De uma forma mais genérica, escrevemos $|x\rangle$ como sendo $|b_n b_{n-1} \dots b_0\rangle$, onde b_i são os dígitos binários do número x.

Para exemplificar um sistema em justaposição, seja H um espaço de Hilbert, e seja $\{|0\rangle, |1\rangle\}$ um base ortonormal selecionada arbitrariamente. Seja $H_{n-1}, H_{n-2}, \dots, H_0$ distintos espaços de Hilbert bidimensionais, cada um com as seguintes bases ortonormais:

$$\{|0_{n-1}\rangle, |1_{n-1}\rangle\}, \{|0_{n-2}\rangle, |1_{n-2}\rangle\}, \dots, \{|0_0\rangle, |1_0\rangle\},$$

respectivamente.

Considere n qubits $Q_{n-1}, Q_{n-2}, \dots, Q_0$ separadamente configurados nos estados

$$\frac{1}{\sqrt{2}}(|0_{n-1}\rangle + |1_{n-1}\rangle), \frac{1}{\sqrt{2}}(|0_{n-2}\rangle + |1_{n-2}\rangle), \dots, \frac{1}{\sqrt{2}}(|0_0\rangle + |1_0\rangle),$$

respectivamente. Q denota o sistema quântico global que consiste dos qubits $Q_{n-1}, Q_{n-2}, \dots, Q_0$ separadamente configurados (sem interação entre eles). Então, o estado $|\psi\rangle$ de Q é o produto tensorial:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_{n-1}\rangle + |1_{n-1}\rangle) \otimes \frac{1}{\sqrt{2}}(|0_{n-2}\rangle + |1_{n-2}\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0_0\rangle + |1_0\rangle).$$

Que é equivalente a:

$$|\psi\rangle = (\frac{1}{\sqrt{2}})^n(|0_{n-1}0_{n-2}\dots 0_1 0_0\rangle + |0_{n-1}0_{n-2}\dots 0_1 1_0\rangle + \dots + |1_{n-1}1_{n-2}\dots 1_1 1_0\rangle).$$

que está no espaço de Hilbert H:

$$H = H_{n-1} \otimes H_{n-2} \otimes \dots H_0.$$

Então, o sistema global Q, que consiste da justaposição dos n qubits $Q_{n-1}, Q_{n-2}, \ldots, Q_0$, está no estado

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^n (|00\ldots00\rangle + |00\ldots01\rangle + \ldots + |11\ldots11\rangle).$$

O exemplo acima é um registrador quântico de n-qubits que contém todos os inteiros de 0 a $2^n - 1$ em sobreposição. Ainda mais importante que isso é o fato de que esse registrador contém todos os inteiros de 0 a $2^n - 1$ *simultaneamente*! Não existe uma analogia na computação clássica para esse fenômeno. Ainda com a definição de registrador quântico em mente, notamos que um sistema de n qubits consegue armazenar 2^n valores distintos. Esse crescimento exponencial do espaço de armazenamento, assim como o armazenamento simultâneo das informações, sugere um possível ganho exponencial de velocidade dos computadores quânticos sobre os computadores clássicos.

Ainda com relação ao exemplo acima, tivemos o primeiro vislumbre do que chamamos de *paralelismo quântico*, ou seja, a sobreposição simultânea de informação. Contudo, há um ponto fraco nisso tudo. Se nós observarmos (medirmos) o registrador, então todo o paralelismo desaparece. Isso porque ao realizarmos uma medição, o estado do registrador necessariamente colapsa em alguma base. Quando medimos, o "mundo quântico" nos seleciona um e somente um dos 2^n possíveis valores. No exemplo acima, a probabilidade de observarmos um número em particular é $\left((1/\sqrt{2})^n\right)^2 = (1/2)^n$. A seleção de qual dos números será escolhido infelizmente não é feita por nós, mas sim pelo "mundo quântico".

4.2 Estados emaranhados

Como vimos acima, um estado está em *justaposição* quando ele pode ser escrito da seguinte forma

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle.$$

Ou seja, se H é um espaço de Hilbert então $|\psi\rangle$ está em justaposição quando $|\psi\rangle$ pode ser escrito como produto tensorial de outros estados que fazem parte de subespaços de H.

Considere agora o estado $|00\rangle + |11\rangle$ (chamado de *par EPR*, devido ao famoso experimento de Einstein, Podolsky e Rosen [30]). Note que esse estado não pode ser descrito como produto tensorial de cada um de seus qubits

separadamente. Em outras palavras, nós não encontramos $\alpha_1, \alpha_2, \beta_1, \beta_2$ tais que

$$(\alpha_1|0\rangle) + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = |00\rangle + |11\rangle.$$

Isso porque

$$(\alpha_1|0\rangle) + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

e $\alpha_1\beta_2 = 0$ implica que ou $\alpha_1\alpha_2 = 0$ ou $\beta_1\beta_2 = 0$. Estados que não podem ser decompostos em produtos tensoriais são chamados *estados emaranhados*[1]. Por ser uma característica marcante dos sistemas quânticos, os estados emaranhados estão enunciados no sétimo princípio da mecânica quântica.

Sétimo Princípio. *Sejam $Q_1, Q_2, \ldots, Q_n$ sistemas quânticos pertencentes aos espaços de Hilbert $H_1, H_2, \ldots, H_n$ respectivamente. Então o sistema quântico global Q, que consiste dos sistemas quânticos $Q_1, Q_2, \ldots, Q_n$ é dito ser* emaranhado *se seu estado $|\psi\rangle \in H = \otimes_{i=1}^{n} H_j$ não pode ser escrito na forma*

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle,$$

onde cada ket $|\psi_i\rangle$ pertence ao espaço de Hilbert H_i, para $i = 0, 1, \ldots, n$. O estado $|\psi\rangle$ também é dito emaranhado.

4.3 Medindo Múltiplos Qubits

Vamos exemplificar a medição de alguns registradores. Devemos lembrar que a medição é probabilística e muda o estado medido fazendo com que o estado medido colapse em alguma base.

Seja o registrador $|R\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ de dois qubits, onde a,b,c e d são números complexos tais que $||a||^2 + ||b||^2 + ||c||^2 + ||d||^2 = 1$. Suponha que queremos medir somente o primeiro qubit (qubit mais à esquerda) com relação à base $\{|0\rangle, |1\rangle\}$. Note que esse é um estado justaposto, pois pode ser escrito como produto tensorial da seguinte forma:

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

$$|R\rangle = |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle).$$

[1]Em algumas referências, os estados emaranhados também são chamados de *estados correlatos*.

Para chegarmos à decomposição completa desse registrador, ainda temos que extrair as amplitudes de probabilidade para o primeiro qubit, ficando:

$$|R\rangle = u|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right) + v|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{c}{v}|1\rangle\right).$$

Para $u = \sqrt{||a||^2 + ||b||^2}$ e $v = \sqrt{||c||^2 + |d|^2}$ os vetores $a/u|0\rangle + b/u|1\rangle$ e $c/v|0\rangle + d/v|1\rangle$ são de tamanho unitário. Uma vez que o estado do registrador foi reescrito da forma acima, fica fácil de observar a probabilidade das medições. Medir o primeiro qubit irá retornar $|0\rangle$ com probabilidade $u^2 = a^2 + b^2$, e irá retornar $|1\rangle$ com probabilidade $v^2 = c^2 + d^2$. Supondo que ao medir o primeiro qubit, obtivemos o resultado $|0\rangle$. Então o estado de $|R\rangle$ ficará $|0\rangle \otimes (a/u|0\rangle + b/u|1\rangle)$. Então, a probabilidade de medir o segundo qubit como $|0\rangle$ é $(a/u)^2$, ou a probabilidade de medir como $|1\rangle$ é $(b/u)^2$.

Supondo agora que temos o par EPR, ou seja, $|R\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Como vimos anteriormente, esse é um estado emaranhado. Como ele não pode ser decomposto como produto tensorial de subespaços, então a medição de um qubit necessariamente modificará outro qubit que ainda não foi medido. Medindo o primeiro qubit, com probabilidade 1/2 conseguimos $|0\rangle$. Automaticamente, o segundo qubit já está definido também como $|0\rangle$, pois não há outra possibilidade de estado que tenha seu primeiro qubit $|0\rangle$. Note a diferença ao medirmos o estado $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$, que não é um estado emaranhado. Ao medirmos o primeiro qubit, esse retorna $|0\rangle$ com probabilidade 1. No entanto, o segundo qubit ainda está indefinido, e pode ser observado tanto como $|0\rangle$ ou como $|1\rangle$ ambos com probabilidade 1/2.

A partir de agora, podemos fazer uma definição alternativa de estados emaranhados. Ao invés de seguir a definição do Sétimo Princípio, podemos pensar que os qubits estão emaranhados se, ao medirmos um qubit, esse causa modifições em algum outro qubit do registrador, assim como medir o primeiro qubit do estado $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ necessariamente causa a definição do segundo qubit. Atenção para não confudir sobre o estado do segundo qubit: após a medição do primeiro qubit, o segundo qubit só pode assumir um valor, mas isso não significa que este foi medido. O que acontece na verdade é que ele está em sobreposição em função do que foi medido no primeiro qubit, mesmo que a sobreposição só leve a um único valor, como no exemplo do par EPR acima. Para ilustar melhor isso, vamos tomar outro exemplo.

Considere o estado $\frac{1}{\sqrt{2^2}}(|000\rangle + |010\rangle + |111\rangle + |101\rangle)$. Supondo que ao observarmos (medirmos) o primeiro qubit, este tenha retornado $|0\rangle$. Observe que o primeiro qubit está emaranhado com o terceiro qubit, então o terceiro qubit assumirá também valor $|0\rangle$. Mas esse ainda não é um qubit medido! Após medirmos o primeiro qubit, o resultado do registrador será

$|0\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. Note também que o estado dos qubits não medidos do registrador está em função dos qubits que já foram medidos. Na prática, porém, na maioria da vezes não há muita diferença em dizer se um qubit está medido ou não se o resultado dele já está definido como 0 ou 1 devido a algum estado emaranhado. No estado acima, por conhecermos de antemão qual a configuração do estado inicial, sabemos que ao medir o primeiro qubit, o terceiro qubit será necessariamente 0, mas geralmente não conhecemos a configuração do estado inicial de uma sobreposição, por isso, para ter certeza que o terceiro qubit será 0, teremos que medi-lo.

4.4 O paradoxo EPR

O paradoxo EPR recebeu este nome porque foi proposto por Einstein, Podolsky e Rosen em 1935 [30]. Ele nos mostra que a mecânica quântica nos leva a conseqüências não esperadas. Esta proposta de experimento foi feita utilizando apenas alguns aspectos teóricos e intuitivos, e na época não imaginava-se que seria possível realizá-lo. O paradoxo EPR propõe a utilização de partículas emaranhadas de uma maneira que parece violar princípios fundamentais da teoria da relatividade.

Suponha uma fonte que produz duas partículas emaranhadas $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Essas duas partículas são chamadas de par EPR. Agora suponha que essas duas partículas afastam-se rapidamente e indefinidamente. Ao efetuarmos uma medição na partícula A, seja qual for a distância entre as duas partículas, a partícula B assumirá o valor medido em A, *instantaneamente*. Isso nos leva a pensar que a mecânica quântica viola o princípio da localidade formulado por Einstein, que diz que mudanças realizadas em um sistema físico não devem ter efeito imediato em outro sistem que está separado no espaço.

O princípio da localidade é convincente, pois parece ser um resultado natural da teoria da relatividade. De acordo com a relatividade, informações não podem ser transmitidas a uma velocidade maior que a da luz, ou o princípio da casualidade (relação causa-efeito) seria violado. Uma análise do paradoxo EPR mostra que a mecânica quântica viola o princípio da localidade sem violar o princípio da casualidade, pois nenhuma informação pode ser transmitida utilizando estados emaranhados. O que pode ser dito é que A e B apenas observarão *um mesmo comportamento aleatório*.

O paradoxo EPR foi a tentativa mais bem sucedida de Einstein contra a mecânica quântica. O objetivo era afirmar que a teoria quântica não é completa, ou seja, que ela é correta (descreve corretamente todas as experiências atualmente concebíveis), porém não descreve todos os fenômenos existentes

no mundo quântico. O paradoxo EPR não foi resolvido ou explicado de uma maneira que atenda à intuição clássica. Ele provocou constantes mudanças na maneira de pensar sobre "o que é a realidade"e "o que é o estado de um sistema físico" além de abrir uma grande discussão sobre a interpretação de Copenhagen, o princípio da localidade e a existência de variáveis ocultas.

Em 1964, após muito tempo da publicação de Einstein, Podolsky e Rosen, John Bell [7] mostrou através de sua inequação que um par de partículas emaranhadas pode ter um comportamento individual aleatório com relações muito fortes para ser explicado pela estatística clássica. Estas correlações foram confirmadas experimentalmente, com fótons e com outras partículas, nos dando uma forte evidencia da validade da mecânica quântica. Outro fato bem conhecido sobre essas correlações entre os pares EPR é que as partículas não podem trocar mensagens significativas e controladas. Antes se pensava que ele só serviria para provar a validade da mecânica quântica. Como veremos adiante, na seção de teletransporte, as partículas podem trocar exatamente a parte da informação de um objeto que é delicada demais para ser escaneada e enviada por meios convencionais.

4.4.1 EPR - Uma analogia

De acordo com o paradoxo EPR, o resultado ao medir uma partícula determina o resultado da medição da outra. Isto ocorre mesmo estas estando distantes uma da outra, como se as duas partículas fossem vistas como um único sistema físico, apesar da distância no espaço.

Imagine que temos duas cartas de baralho, sendo uma delas um rei e a outra uma dama, ambas com a face desenhada virada para baixo. Agora viramos a primeira carta. Olhando para ela, o que podemos concluir? Que se a carta que viramos é o rei, a outra carta é necessariamente a dama, ou o contrário. Na mecânica quântica estas cartas não teriam valor algum quando estivessem viradas para baixo, pois estariam em uma sobreposição de estados. A carta assume um valor apenas quando a viramos, ou fazemos uma "medição". Com esta medição feita, determinamos o valor da outra, pois as duas não podem ser a mesma carta. Note que mesmo com uma das cartas viradas, a outra continua não tendo valor. Esta só assumirá o valor determinado pela carta que já foi virada quando for observada.

Capítulo 5

Portas

Em 1985, Deutsch [17] propôs o modelo original de computação quântica, que era basicamente uma máquina de Turing, mas com a adição de algumas propriedades as quais permitiam que as células da fita e a cabeça de leitura/escrita poderiam estar numa sobreposição quântica. Deutsch também definiu as funções de transição, que deveriam se preocupar com que as trasformações na máquina de Turing fossem transformações unitárias. Tudo isso contribuía para um modelo muito mais difícil de se programar em comparação com as máquinas de Turing clássicas, que também já requerem um trabalho tedioso. Verificar na máquina de Turing quântica que uma dada função de transição corresponde a uma transformação unitária não é nada trivial. Bernstein e Vazirani propuseram algumas regras para verificar se uma transformação na MT quântica de fato é unitária, mas ainda assim, trabalhar com o modelo de MT despende muito trabalho.

Na teoria da complexidade clássica, o modelo computacional de circuitos é comumente utilizado. O modelo de circuitos é equivalente ao modelo de MT clássica no que diz respeito às capacidades de computar desses dois modelos, que podem simular um ao outro com uma sobrecarga de ordem polinomial. Isso faz com que a escolha de uso de um ou de outro modelo seja uma mera questão de gosto.

O modelo de circuitos quânticos, que utiliza portas quânticas (assim como no caso clássico utilizam-se as portas lógicas) também é equivalente ao modelo da MT quântica. Computacionalmente falando, a escolha de algum desses dois modelos para uso não faz diferença. Contudo, como as portas quânticas permitem uma maneira mais natural de tratar a unitariedade da transformações, o modelo de circuitos quânticos (que utiliza as portas quânticas) está se tornando o modelo padrão para a computação quântica, ou seja, é o modelo mais utilizado.

5.1 Transformações Unitárias

As situações vistas até agora são consideradas *estáticas* no sentido que os estados iniciais não sofreram mudanças (com exceção das mudanças de estados quando se realiza uma medição) após terem sido configurados.

O princípio fundamental na mudança de estados em um sistema quântico são as transformações unitárias. Uma transformação unitária é uma transformação linear que é inversível e cuja inversa é igual a sua conjugada transposta. Ou seja, a matriz U é unitária se

$$UU^* = U^*U = I,$$

onde U^* é a conjugada transposta de U e I é a matriz identidade. As transformações unitárias são inerentes a qualquer sistema quântico dinâmico, i.e., sistemas que sofrem mudanças em seus estados. As transformações unitárias podem ser vistas como uma característica de mecânica quântica, devido à sua grande importância em todas operações modificadoras de um sistema. Assim sendo, isso é colocado como mais um princípio:

Oitavo Princípio. *Vetores de estado são transformados por matrizes unitárias.*

Intuitivamente falando, a transformação unitária corresponde a uma rotação no espaço vetorial que preserva o mesmo comprimento do vetor e a mesma quantidade de informação do sistema. A preservação do comprimento do vetor garante que a probabilidade total de um conjunto de estados sempre permaneça igual (1 se considerarmos o qubit normalizado) e que a norma do vetor não extrapole os limites da esfera de Bloch. A preservação de informação reflete o princípio universal da conservação com relação a sistemas físicos quânticos que estabelece que todas as mudanças em nível microscópico preservam a informação. Em outras palavras, o estado quântico (vetor de amplitudes) de um sistema isolado pode determinar (probabilisticamente) a qualquer momento o estado quântico do sistema no passado e no futuro.

A porta clássica mais simples é a porta NOT, que é uma porta de um bit que nega o estado do bit de entrada: 0 vira 1 e vice-versa. A porta quântica correspondente é implementada via uma operação unitária que faz com que os estados-base mudem seus estados de acordo com a tabela-verdade do NOT clássico. Seja U_{not} a operação quântica unitária que corresponde ao NOT clássico. Essa operação, aplicada a um estado, poderia ser descrita como

$$U_{\text{not}}(|0\rangle) = |1\rangle,$$
$$U_{\text{not}}(|1\rangle) = |0\rangle.$$

Na computação clássica, as portas sempre retornam 0 ou 1, por isso são chamadas de portas lógicas. Na computação quântica, as portas não precisam necessariamente retornar 0 ou 1, e a noção de porta pode ser extendida para operações que não têm uma analogia na computação clássica. Por exemplo, seja U_A uma operação descrita abaixo.

$$U_A(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$U_A(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Essa operação define um estado quântico válido, no entanto, não existe um caso análogo na computação clássica.

5.2 Portas simples

Abaixo vamos mostrar algumas portas bem simples. Algumas são utilizadas com frequência, outras não são muito utilizadas mas ilustram bem o funcionamento das portas quânticas. Note que todas as portas a serem descritas são matrizes unitárias (que realizam transformações unitárias).

5.2.1 NOT

A operação da porta NOT como já foi explicada, é definida pela sua tabela-verdade $0 \to 1$ e $1 \to 0$. A matriz de transformação dessa operação é dada por

$$U_{\text{not}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Supondo que $|0\rangle$ e $|1\rangle$ sejam definidos como os vetores $(1,0)^T$ e $(0,1)^T$ respectivamente, então a operação de NOT funciona da seguinte maneira

$$U_{\text{not}}(|0\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

Analogamente podemos aplicar U_{not} para $|1\rangle$.

5.2.2 Inversão de fase

A matriz de transformação dessa operação é dada por

$$U_i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

cuja função é levar um estado $\alpha|0\rangle + \beta|1\rangle$ para $\alpha|0\rangle - \beta|1\rangle$.

5.2.3 Hadamard-Walsh

Uma das mais importantes portas da computação quântica, a porta Hadamard não tem uma função análoga na computação clássica. Sua matriz é dada por

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Sua função é a seguinte

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Quando a porta H é aplicada a mais de um qubit, chamamos essa transformação de Walsh, ou Walsh-Hadarmard. Ela pode ser definida recursivamente como

$$\begin{cases} W_1 &= H, \\ W_{n+1} &= H \otimes W_n. \end{cases}$$

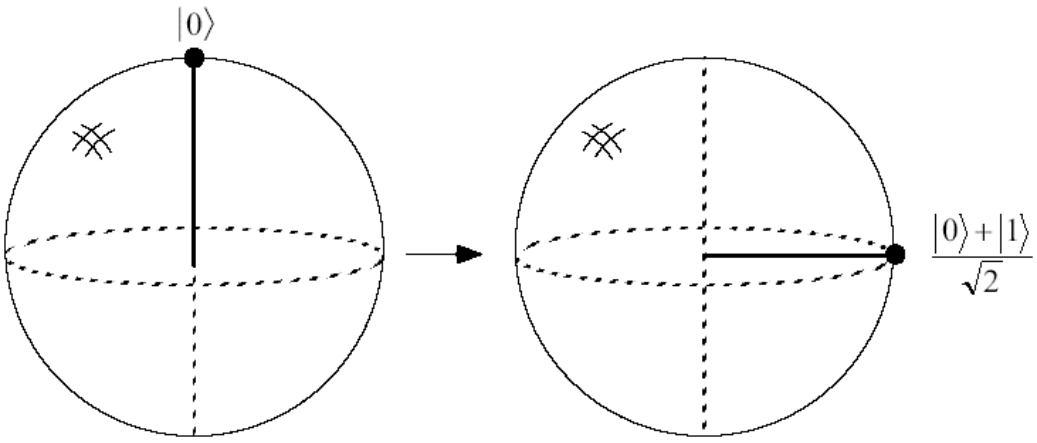


Figura 5.2.1: Representação geométrica da porta Hadamard aplicada ao estado $|0\rangle$.

Ou seja, a porta H é aplicada em todos os qubits de um registrador. Essa transformação é de grande utilidade: seja $|\psi\rangle$ um registrador inicialmente configurado com todos os seus qubits em $|0\rangle$. Aplica-se a porta H em cada

qubit separadamente, então o resultado fica

$$\begin{aligned}|\psi\rangle &= H \otimes H \otimes \ldots \otimes H|00\ldots0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \ldots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \Big(\frac{1}{\sqrt{2}}\Big)^n (|00\ldots0\rangle + |00\ldots1\rangle + \ldots + |11\ldots1\rangle) \\ &= \Big(\frac{1}{\sqrt{2}}\Big)^n \sum_{i=0}^{2^n-1} |i\rangle.\end{aligned}$$

Em outras palavras, ao aplicar a transformação Walsh-Hadamard num registrador inicialmente configurado em $|00\ldots0\rangle$, conseguimos uma sobreposição de todos os valores possíveis de ser armazenados nesse registrador. Além disso, com um número linear de operações (i.e, para um registrador de n qubits, aplicamos a porta Hadamard n vezes), geramos um estado no registrador que contém um número exponencial (2^n) de termos distintos, em outras palavras, o registrador contém todos os valores numéricos de tamanho n possíveis em sobreposição e com a mesma amplitude. Em contraste com o caso clássico, num registrador de n bits, podemos armazenar somente um único valor numérico em cada estado.

Em geral, há infinitas portas para um único qubit, todas elas podem ser generalizadas como *rotações*,

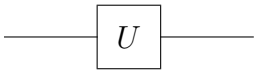
$$U_R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

e *deslocamentos de fase*,

$$U_P(\phi_1, \phi_2) \begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & e^{i\phi_2} \end{pmatrix}.$$

Fica simples imaginar as rotações e deslocamentos de fase quando pensamos no modelo geométrico 3D do qubit (esfera de Bloch).

As portas simples também são representadas graficamente como:



Onde U é um *rótulo* para descrever a função da porta. Por exemplo, para a porta Hadamard, um exemplo de rótulo poderia ser H. Essas representações são usadas para representar graficamente a construção de circuitos mais complexos que utilizam a combinação de portas simples para realizar operações não triviais, como, por exemplo, montar um circuito que realiza adição.

5.3 Portas de múltiplos qubits

Para construir circuitos quânticos não triviais é necessário a inclusão de operações que manipulam mais de um qubit. Nas portas clássicas para múltiplos bits, as portas AND e OR se destacam como sendo as principais portas da computação clássica. Vamos mostrar algumas portas quânticas de múltiplos qubits, entre elas, as portas que simulam operações clássicas como AND e SWAP.

5.3.1 NOT-Controlado

A porta NOT-Controlado (abreviada como C-NOT) têm seu funcionamento descrito pelo diagrama da Figura 5.3.2.

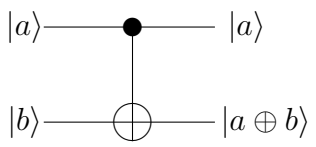


Figura 5.3.2: Notação para a porta NÃO-CONTROLADO (C-NOT).

Onde $\oplus$ é a operação de ou-exclusivo (XOR). Entra o estado $|a\rangle$ e sai o estado $|a\rangle$. Por outro lado, entra o estado $|b\rangle$, e sai como estado $|a \oplus b\rangle$.

Mas uma maneira diferente de interpretar esse diagrama é dizer que o qubit $|a\rangle$ é um sinal de controle para especificar se devemos ou não negar o qubit $|b\rangle$. Em outras palavras, se o qubit $|a\rangle$ estiver "ligado", o qubit $|b\rangle$ é negado. Se $|a\rangle$ estiver desligado, $|b\rangle$ não é modificado. Essa transformação é dada pela matriz[1]

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

A porta C-NOT é uma porta muito importante para a composição de operações mais complexas. Como exemplo, vamos construir um circuito composto de C-NOT's que troca um par de qubits que estão na base computacional, descrito no diagrama abaixo.

[1]Assumindo que $|00\rangle$, $|01\rangle$, $|10\rangle$, e $|11\rangle$ estão associados a $(1,0,0,0)^T$, $(0,1,0,0)^T$, $(0,0,1,0)^T$ and $(0,0,0,1)^T$, respectivamente.

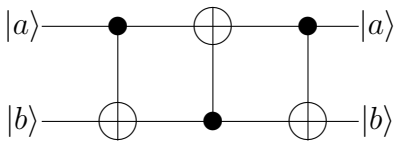


Figura 5.3.3: Circuito que simula um SWAP.

A ação do circuito é

$$|a,b\rangle \to |a, a\oplus b\rangle \to |(a\oplus b)\oplus a, a\oplus b\rangle = |b, a\oplus b\rangle \to |b, b\oplus(a\oplus b)\rangle = |b,a\rangle\,.$$

5.3.2 Porta Toffoli

Similarmente à porta C-NOT, a porta Toffoli nega o terceiro qubit se e somente se os dois primeiros qubits são 1. A representação gráfica da porta Toffoli é

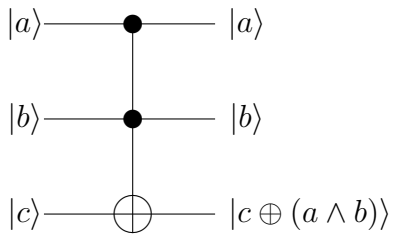


Figura 5.3.4: Notação para a porta Toffoli (C^2-NOT).

A porta Toffoli também pode ser utilizada para computarmos uma operação de AND. Se inicializarmos $|c\rangle$ com 0, o estado final do terceiro qubit é $|a\wedge b\rangle$. Essa porta também é chamada de NOT-Controlado-Controlado ou sua abreviação, C^2-NOT.

5.4 Computação reversível

Uma importante consequência do fato das transformações quânticas serem unitárias é que elas são *reversíveis*. Ou seja, como todos operadores unitários U são inversíveis aplicando $U^{-1} = U^*$, podemos sempre "descomputar" (reverter a computação) em um computador quântico. Computadores clássicos,

por outro lado, são expressos em termos de passos que não são reversíveis. Por exemplo, não é possível recuperar a entrada depois de aplicar a porta clássica AND.

Em circuitos irreversíveis, tomando como exemplo a porta AND, há duas entradas mas somente uma saída. Implicitamente nesses circuitos, há uma operação ERASE, que apaga um dos bits de entrada. O problema é que quando um sistema computacional apaga um bit de informação, é liberada energia em forma de calor, fazendo com que os circuitos aqueçam demais. A Lei de Moore [27] estabelece um crescimento exponencial da velocidade dos computadores através do tempo. Mas essa lei está com os dias contados. Isso porque, para o aumento exponencial da velocidade, é necessário que os circuitos sejam construídos cada vez menores. Mas há um limite em tornar os circuitos menores devido a duas barreiras: por um lado, se conseguirmos controlar o aquecimento, iremos esbarrar em circuitos de dimensões tão pequenas que não obedecerão à leis da mecânica clássica, mas sim às leis da mecânica quântica. Por outro lado, podemos nem chegar perto da barreira de tamanho da mecânica quântica devido aos circuitos super-aquecerem. Resumindo, a evolução natural dos sistemas computacionais físicos tende a considerar componentes cada vez menores, que serão tratados pela computação quântica, e devem ser livres do aquecimento dos componentes, que é tratado pela reversibilidade. Estudos dizem que a Lei de Moore irá se manter até aproximadamente o ano de 2015.

Apesar da reversibilidade ser inerente à unitariedade, um computador quântico *necessita* ter de operar reversivelmente. Isso porque se os circuitos quânticos receberem calor, eles simplesmente "derretem" (os qubits mudam de estados arbitrariamente) devido ao seus tamanhos. A vantagem dos circuitos reversíveis é que eles não liberam calor, pois não há operações de ERASE: a quantidade de qubits que entram é a mesma quantidade de qubits que saem da transformação.

5.5 Teorema da não-clonagem

Seria possível criar uma combinação de circuitos quânticos mais complicada que conseguisse copiar estados quânticos arbitrários? A resposta é não, como afirmado anteriormente, é impossível clonar um estado quântico. É fácil de verificar que a clonagem é impossível de ser realizada usando uma medição desse estado. Isso porque, para clonar um estado, deveríamos realizar uma medição nesse, no entanto, ao realizar a medição, podemos ter criado um qubit clone, mas o qubit original irá colapsar devido à medição feita. Qualquer

outro método utilizado para tentar clonar qubits também seria uma tentativa fadada ao fracasso devido ao Teorema da Não-Clonagem descrito abaixo.

Teorema da Não-Clonagem. *Seja $|\psi\rangle$ um estado. Não existe uma tranformação unitária U tal que*

$$U(|\psi 0\rangle) = |\psi\psi\rangle.$$

Prova. Suponha que exista U tal que:

$$U(|\psi 0\rangle) = |\psi\psi\rangle,$$

$$U(|\phi 0\rangle) = |\phi\phi\rangle,$$

para quaisquer ψ,ϕ. U estaria representando a suposta operação de clonagem. Considere $|\varphi\rangle = (1/\sqrt{2})(|\psi\rangle + |\phi\rangle)$. Então, por linearidade:

$$\begin{aligned} U(|\varphi 0\rangle) &= \frac{1}{\sqrt{2}}\Big(U(|\psi 0\rangle) + U(|\phi 0\rangle)\Big) \\ &= \frac{1}{\sqrt{2}}\Big(|\psi\psi\rangle + |\phi\phi\rangle\Big). \end{aligned}$$

Mas se U é uma tranformação de clonagem, então:

$$U(|\varphi 0\rangle) = |\varphi\varphi\rangle = \frac{1}{2}\Big(|\psi\psi\rangle + |\psi\phi\rangle + |\phi\psi\rangle + |\phi\phi\rangle\Big).$$

□

É importante entender que os qubits cujos estados quânticos são conhecidos são fácilmente clonáveis, pois já estão colapsados em alguma base, e qualquer medição realizada não irá mudar seu estado, ou seja, é análogo a copiar (clonar) bits clássicos. O que o Teorema da Não-Clonagem realmente nos diz é que não há como clonar qubits cujos estados quânticos sejam desconhecidos.

Capítulo 6

Funções

Agora vamos começar a entender como funções são executadas em um computador quântico. Considere a função

$$f : \{0, 1, \ldots, 2^m - 1\} \rightarrow \{0, 1, \ldots, 2^n - 1\}$$

onde m e n são inteiros positivos. Um computador clássico iria processar cada uma das entradas $0, 1, \ldots, 2^m - 1$ em suas respectivas saídas, $f(0), f(1), \ldots, f(2^n - 1)$. Em um computador quântico, as funções são computadas de uma maneira diferente, devido basicamente a unitariedade e reversibilidade das transformações. Note que, no computador quântico, não é possível computar uma função f por uma operação unitária que leva $|x\rangle$ para $|f(x)\rangle$. Isso porque se f não é um mapeamento um-para-um (i.e, $f(x) = f(y)$ para $x \neq y$), então dois kets ortogonais distintos $|x\rangle$ e $|y\rangle$ podem levar ao mesmo ket $|f(x)\rangle = |f(y)\rangle$ como resultado, violando a unitariedade.

Uma maneira de computar funções que não são de mapeamento um-para-um, preservando a reversibilidade da computação, é armazenar a entrada separadamente da saída. Para isso, temos que tratar um registrador como se fossem dois registradores distintos: a primeira parte do registrador armazena a entrada, e a segunda parte armazena a saída. Cada entrada possível para x é representada como $|x\rangle$, que é o estado da primeira parte do registrador. Analogamente, a saída $f(x)$ é representada como $|f(x)\rangle$, que é o estado da segunda parte do registrador. Inicialmente, o registador é denotado por

$$|\psi\rangle = |x\rangle|0\rangle.$$

A segunda parte do registrador é inicializada com $|0\rangle$ antes de ser computada. A avaliação da função é então determinada pelo operador de transformação unitária U_f que age em ambos os registradores

$$U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle.$$

Note que eliminamos o problema de funções que levam a mapeamentos que não são um-para-um. Isso porque, se $|x\rangle$ leva a $|f(x)\rangle$ e $|y\rangle$ também leva a $|f(x)\rangle$, o estado do registrador no primeiro caso será $|\psi_1\rangle = |x\rangle|f(x)\rangle$ que é diferente de $|\psi_2\rangle = |y\rangle|f(x)\rangle$, ou seja, os dois estados não são mais representados pelo mesmo vetor no espaço de Hilbert.

As computações com que estamos trabalhando aqui, além de serem reversíveis, também são quânticas. Isso indica que, devido a característica da sobreposição, podemos fazer muito mais que ficar computando valores um a um. Podemos utilizar a transformação Walsh-Hadamard para configurar uma sobreposição de todos os valores de entrada possíveis num único estado, e ao executar a computação de U_f *somente uma vez*, todos os 2^m valores de $f(0), f(1), \ldots, f(2^m - 1)$ são computados

$$|\psi\rangle = U_f\Big(\frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|0\rangle\Big) = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|f(x)\rangle.$$

Como era de se esperar, não existe uma medição quântica que consiga extrair os 2^m valores $f(0), f(1), \ldots, f(2^m - 1)$ do estado $|\psi\rangle$. Imagine, por exemplo, que vamos realizar uma medição na primeira parte (as entradas $|x\rangle$) do registrador $|\psi\rangle$. A mecânica quântica nos permite inferir sobre os seguintes fatos:

- Como cada valor x aparece com a mesma amplitude (portanto, com a mesma probabilidade) na primeira parte do registrador, então as saídas de uma medição têm a mesma probabilidade e pode ser qualquer um dos valores de $f(0), f(1), \ldots, f(2^m - 1)$.

- Considerando que um resultado de uma medição na primeira parte do registrador é $|j\rangle$, então o estado de *pós-medição* do registrador considerando as duas partes é $|\psi\rangle = |j\rangle|f(j)\rangle$. Então uma medição subsequente na segunda parte do registrador irá levar certamente ao resultado $f(j)$, e nenhuma informação adicional sobre f pode ser obtida.

Contudo, há casos de funções periódicas em que $f(j)$ pode retornar mais de um resultado. Por exemplo, seja o pseudo-código

```
fun(a){
   retorna x tal que (sen(x) == a)
}
```

Onde a é uma constante fornecida à função. Como a função seno é uma função periódica, se entrarmos com $a = 1$, então essa função irá retornar

todos os ângulos cujo o seno é 1. Ou seja, há mais de um resultado de retorno possível. Voltando ao nosso exemplo do registrador dividido em duas partes, se aplicarmos nesse registrador a função *fun* descrita acima e ao realizar a medição na primeira parte do registrador obtemos o valor 1, então a segunda parte irá conter os ângulos x que cujo seno é igual a 1[1]. Em outras palavras, o resultado (segunda parte do registrador) conterá vários valores em função do valor que foi medido na primeira parte do registrador. Obviamente, se medirmos a segunda parte do registrador, a sobreposição acaba e teremos somente um resultado. Essa característica será bem ilustrada na explicação da fatoração quântica (algoritmo de Shor), que utiliza esse artifício para encontrar o período de uma função.

6.1 Dense Coding

Dense coding utiliza um bit quântico junto com um par EPR para codificar e transmitir dois bits clássicos. Desta maneira, somente um bit precisa ser fisicamente transmitido para comunicar dois bits de informação. Para isso, Alice e Bob precisam de um par EPR, onde cada um recebe um bit do par emaranhado

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Utilizaremos 4 transformações: I (identidade), 2 transformações já vistas (U_{not} e U_i) e $\mathrm{Y} = U_i U_{\text{not}}$:

$$\begin{array}{lrcll}
I: & |0\rangle & \rightarrow & |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
 & |1\rangle & \rightarrow & |1\rangle & \\
U_{\text{not}}: & |0\rangle & \rightarrow & |1\rangle & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 & |1\rangle & \rightarrow & |0\rangle & \\
U_i: & |0\rangle & \rightarrow & |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
 & |1\rangle & \rightarrow & -|1\rangle & \\
Y: & |0\rangle & \rightarrow & -|1\rangle & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
 & |1\rangle & \rightarrow & |0\rangle &
\end{array}$$

Alice tem 2 bits que deve transmitir para Bob, codificando os números de 0 a 3. Dependendo desse número, Alice aplica uma das transformações $\{I, U_{\text{not}}, U_i, Y\}$ em seu qubit do par emaranhado ψ_0. Ao primeiro bit será

[1]Sabemos que há infinitos ângulos satisfazendo essa propriedade, no entanto, podemos representar somente um número finito de ângulos. O tamanho do registrador limita a quantidade de ângulos representáveis.

aplicada a transformação escolhida, enquanto que ao segundo será aplicada a transformação identidade. O estado resultante é mostrado abaixo:

Valor	Transformação	Novo estado
0	$\psi_0 = (I \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$\psi_1 = (U_{\text{not}} \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$\psi_2 = (Y \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
3	$\psi_3 = (U_i \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Então Alice envia seu qubit para Bob. Bob aplica a transformação de NOT-controlado nos dois qubits do par EPR.

Estado Inicial	NOT-Controlado	Primeiro bit	Segundo bit
$\psi_0 = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$\psi_1 = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\psi_2 = \frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\psi_3 = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|0\rangle$

Note que agora Bob pode medir o segundo qubit sem alterar o estado quântico. Se a medição retornar $|0\rangle$, então o valor codificado ou é 0 ou é 3. Por outro lado, se a medição retornar $|1\rangle$, então o valor codificado ou é 1 ou 2.

Agora Bob aplica H (Hadamard) ao primeiro bit:

Estado Inicial	Primeiro bit	H(Primeiro bit)
ψ_0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}\big(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\big) = \|0\rangle$
ψ_1	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}\big(\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\big) = \|0\rangle$
ψ_2	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}\big(-\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\big) = \|1\rangle$
ψ_3	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}\big(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) - \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\big) = \|1\rangle$

Finalmente, Bob mede o bit resultante, o qual permite distinguir entre 0 e 3, e 1 e 2.

6.2 Teletransporte

Teletransporte é o nome criado pela ficção científica para o fato de fazer um objeto ou uma pessoa desaparecer de um lugar e aparecer em outro, perfeitamente igual ao original. Como isso é feito sempre ficou obscuro para os telespectadores (e também para os autores), obviamente porque isso é, ou era, apenas ficção. Os autores usam a intuição para simular este acontecimento:

1. O objeto é varrido de tal forma que se obtivesse toda a informação relativa a ele.

2. Essa informação é transmitida de alguma forma até o seu destino.

3. Finalmente, com a informação recebida, o objeto é reconstituído no local desejado.

Note que o que é levado ao destino é a informação sobre o objeto, e não seus componentes físicos. Assim podemos concluir que o objeto que aparece no destino é uma cópia exata, e não o mesmo objeto que estava na posição inicial. Essa réplica não é constituída da mesma matéria do original, mas sim de átomos do mesmo tipo, organizados exatamente da mesma maneira.

Em 1993 um grupo internacional da IBM composto por 6 cientistas mostrou que o teletransporte é de fato possível de ser realizado, mas somente se o objeto original for destruído. Não poderíamos fazer várias cópias de um mesmo objeto ou pessoa, a partir do momento em que o estado original é sempre destruído para que seja possível ler todas as informações relativas a ele. Então, outros cientistas começaram a planejar experimentos para demonstrar o teletransporte de objetos microscópicos, como um átomo ou um fóton. Entretanto, ninguém espera ser possível teletransportar pessoas ou outros objetos macroscópicos em um futuro próximo, ainda que isso não viole nenhuma lei fundamental.

No princípio, o teletransporte era considerado uma utopia. Ele não era levado a sério porque se pensava que violaria o princípio da incerteza da mecânica quântica, o qual proíbe qualquer tipo de medição de extrair toda a informação de um átomo. De acordo com o princípio da incerteza, quanto mais exata a medição de um objeto, mais seu estado é perturbado pelo processo de medição, até atingir um ponto onde o estado original do objeto estaria completamente desorganizado. E esse ponto ocorreria antes mesmo de se conseguir informações suficientes para fazer uma réplica exata.

Como contornar este problema? A resposta está no paradoxo EPR. O grupo de cientistas da IBM encontrou uma maneira de varrer parte da informação do objeto A, o qual queremos teletransportar, e transmití-la através de meios clássicos, e a parte não varrida da informação transmitir através do efeito EPR, a um outro objeto C que nunca esteve em contato com A. Após isso, é possível manipular o objeto C de forma que este fique no estado exato em que A se encontrava ao ser teletransportado. A informação sobre o objeto A é levada até C por um outro objeto B. Este objeto B é na verdade

um par EPR, ou seja, é um par de partículas emaranhadas.

Como vimos, o objetivo do teletransporte é transmitir o estado quântico de uma particula utilizando bits clássicos e um par EPR e reconstruir o estado quântico *exato* no destino. Também sabemos que um estado quântico não pode ser copiado, pois isso violaria o teorema da não-clonagem. Isso significa que o estado original deve ser necessariamente destruído. O teletransporte de um bit único foi realizado experimentalmente [13].

Alice e Bob irão realizar este teletransporte. Cada um recebe um bit do par EPR

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Alice tem um qubit ϕ, e ela não conhece o estado desse qubit.

$$\phi = \alpha|0\rangle + \beta|1\rangle.$$

Alice aplica o passo de decodificação do *dense coding* a esse qubit e à sua metade do par emaranhado. Então temos inicialmente o seguinte estado:

$$\begin{aligned} \phi \otimes \psi_0 &= \frac{1}{\sqrt{2}}\big(\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|00\rangle + |11\rangle)\big) \\ &= \frac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\big), \end{aligned}$$

dos quais Alice controla os dois primeiros bits, e Bob o último. Agora, Alice aplica $U_{\text{not}} \otimes I$ e $H \otimes I \otimes I$ a esse estado:

$$\begin{aligned} &(H \otimes I \otimes I)(U_{\text{not}} \otimes I)(\phi \otimes \psi_0) \\ &= (H \otimes I \otimes I)(U_{\text{not}} \otimes I)\frac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\big) \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\big) \\ &= \frac{1}{2}\big(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\big) \\ &= \frac{1}{2}\big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\big). \end{aligned}$$

Alice faz uma medição nos dois primeiros qubits e tem como resultado um dos seguintes estados:

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle,$$

com igual probabilidade.

Dependendo do resultado da medição, o estado quântico do qubit de Bob é projetado para:

$$\alpha|0\rangle + \beta|1\rangle,\ \alpha|1\rangle + \beta|0\rangle,\ \alpha|0\rangle - \beta|1\rangle,\ \alpha|1\rangle - \beta|0\rangle,$$

respectivamente. Alice envia o resultado da sua medição como dois bits clássicos para Bob.

Note que quando Alice fez a medição, ela alterou irreversivelmente o estado de seu qubit original ϕ, que está em processo de envio para Bob. Essa é a razão pela qual o teletransporte não viola o princípio de não-clonagem.

Quando Bob recebe os dois bits clássicos de Alice, ele sabe como o estado da sua metade do par emaranhado se compara ao estado original do qubit de Alice.

bits recebidos	estado	decodificação
00	$\alpha\|0\rangle + \beta\|1\rangle$	I
01	$\alpha\|1\rangle + \beta\|0\rangle$	U_{not}
10	$\alpha\|0\rangle - \beta\|1\rangle$	U_i
11	$\alpha\|1\rangle - \beta\|0\rangle$	Y

Bob consegue reconstruir o estado original do qubit ϕ de Alice aplicando a transformação de decodificação apropriada à sua parte do par EPR. Note que esse é o passo de codificação no *dense coding*.

O teletransporte quântico é teoricamente perfeito, gerando um estado de saída que é igual ao estado de entrada com fidelidade 1. Na prática (o teletransporte já foi realizado em laboratórios), resultados com fidelidade menores que 1 ocorrem devido a imperfeições no par EPR, na medição de Alice, e na transformação unitária de Bob. Se for utilizado apenas um meio clássico não há esperanças de se transferir um estado quântico arbitrário com fidelidade 1. No teletransporte "clássico" o limite de fidelidade é 0.5, enquanto a fidelidade no teletransporte quântico foi determinada experimentalmente como sendo igual a 0.58. Note que esta fidelidade é uma média sobre todos os estados da entrada, então ela mede a habilidade de se transferir de Alice para Bob uma sobreposição arbitrária e desconhecida.

Capítulo 7

Algoritmo de Shor

7.1 Introdução

Em 1994, Peter Shor descreveu um algoritmo quântico que resolve o problema da fatoração em primos em tempo polinomial. Esse algorimo foi batizado como "Algoritmo de Shor" e é o mais importante resultado obtido até agora na computação quântica. O resultado de Shor foi o principal motivo que alavancou o interesse do estudo da computação quântica ao redor do mundo.

Desde Euclides, sabemos que todo número inteiro positivo N pode ser fatorado em um produto de números primos. Além disso, é relativamente fácil descobrir se um dado número é primo ou não. Isso pode ser feito em tempo $O(\log^{12} n)$ com o teste de primalidade AKS [31], descoberto no ano de 2002. Contudo, dado um número composto, é difícil descobrir os seus fatores primos. O algoritmo de Shor é considerado importante por conseguir vencer a dificuldade que há em encontrar os fatores primos de números grandes. Por esta dificuldade os números primos são utilizados pela maioria dos sistemas de criptografia, no entanto, se um eficiente método de fatorar números grandes for descoberto, a maioria dos esquemas atuais de criptografia será comprometida. Enquanto não for publicado um algoritmo que fatore números grandes em tempo polinomial para um computador clássico, a criptografia está segura, pois o algoritmo mais eficiente conhecido roda em tempo $O(e^{c(\log n)^{1/3}(\log\log n)^{2/3}})$ ou seja, é exponencial no tamanho da entrada.

O algoritmo de Shor é executado em parte num computador clássico e parte num computador quântico rodando $O((\log n)^2 \log\log n)$ passos no computador quântico e $O(\log n)$ passos no computador clássico.

7.2 Visão geral do algoritmo

Os mais eficientes algoritmos clássicos que resolvem o problema da fatoração utilizam o fato de que o problema da fatoração pode ser reduzido ao problema de encontrar o período de uma função periódica. O algoritmo de Shor também utiliza essa redução.

Seja a função $F(a) = x^a \mod N$, onde x é um inteiro co-primo[1] a N. A razão porque essa função é útil para fatorar números grandes é que $F(a)$ é uma função que tem um período r. Dessa forma, como $x^0 \mod N = 1$, então $x^r \mod N = 1$ e $x^{2r} \mod N = 1$ e assim por diante. Sabendo disso, temos

$$\begin{aligned} x^r &\equiv 1 \mod N \\ &\Updownarrow \\ (x^{r/2})^2 &\equiv 1 \mod N \\ &\Updownarrow \\ (x^{r/2})^2 - 1 &\equiv 0 \mod N. \end{aligned}$$

E, se tivermos a sorte do período r ser um número par, então

$$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \mod N.$$

Podemos ver que o produto $(x^{r/2}-1)(x^{r/2}+1)$ é um inteiro múltiplo de N (pois o resto da divisão é igual a 0), onde N é o número a ser fatorado. Se $x^{r/2}$ não é igual a ± 1 e r é par, então ao menos um dos termos $(x^{r/2}-1)$ e $(x^{r/2}+1)$ deve ser um fator não-trivial de N. Assim, ao computar $\text{mdc}(x^{r/2} - 1, n)$ e $\text{mdc}(x^{r/2} + 1, n)$, nós obteremos pelo menos um fator de N, onde *mdc* é a função do máximo divisor comum.

Essa é uma breve descrição do algoritmo de Shor que será explicado com maiores detalhes nas próximas seções:

1. N é o número a ser fatorado;
2. x é co-primo a N e $x \in \{0, 1, \ldots, N-1\}$;
3. Determine o período r tal que $x^r \equiv 1 \mod N$;
4. Um fator de N é o $\text{mdc}(x^{r/2} - 1, N)$ e/ou $\text{mdc}(x^{r/2} + 1, N)$.

[1] Números *co-primos* são número *primos entre si*, ou seja, o máximo divisor comum entre eles é 1.

O algoritmo de Shor tenta achar r, que é o período da função periódica $F(a) = x^a \mod N$, onde N é o número a ser fatorado, x é um inteiro co-primo de N.

Para fazer isso o algoritmo de Shor cria um registrador quântico com duas partes, como:

$$|\psi\rangle = |0\rangle|0\rangle.$$

Na primeira parte do registrador, o algoritmo coloca uma sobreposição de inteiros os quais são os a's da função $x^a \mod N$. Serão escolhidos os a's para serem inteiros 0 até $q-1$, onde q é potência de dois, tal que $N^2 \leq q \leq 2N^2$. Então o algoritmo calcula $x^a \mod N$, onde a é a sobreposição dos estados, e coloca o resultado na segunda parte do registrador quântico.

Após isso, o algoritmo mede o estado da segunda metade do registrador, que contém a sobreposição de todos os possíveis resultados da função $x^a \mod N$. Ao medir esse registrador, o estado colapsa em algum valor fixo, que chamaremos de k. Ao medir a segunda parte do registrador quântico, esse é projetado (colapsa) em k e então a primeira parte do registrador estará numa sobreposição de valores em função do valor k que foi medido. Como $F(a) = x^a \mod N$ é uma função periódica, sabe-se que a primeira parte do registrador irá conter o valor $c, c+r, c+2r \ldots$ e assim por diante, onde c é o menor inteiro tal que $x^c \mod N = k$.

O próximo passo é executar uma transformada quântica de Fourier na primeira parte do registrador e colocar o resultado novamente nessa parte. A função da transformada de Fourier será explicada com mais detalhes na próxima seção. Por hora basta saber que, após a aplicação da transformada de Fourier, o estado quântico da primeira parte do registrador estará em sobreposição *somente* dos valores múltiplos de q/r.

Então, ao medir a primeira parte do registrador quântico, obteremos v, que é um inteiro múltiplo de q/r. A partir daí, podemos utilizar o valor v no computador clássico, para computar o período r, e então conseguirmos um fator de N.

7.3 Transformada quântica de Fourier

A *transformada de Fourier* mapeia funções do domínio do tempo para o domínio da freqüência. Informalmente falando, a transformada de Fourier mapeia funções com período r para funções que possuem valores diferentes de zero apenas nos múltiplos da freqüência $2\pi/r$. A *transformada discreta de Fourier* (DFT), por sua vez, opera em q pontos igualmente espaçados no intervalo, por isso ela é chamada de discreta. A transformada discreta de Fourier de uma função com o período r é uma função concentrada perto dos

múltiplos de q/r, ou seja, a função é diferente de zero somente nos valores próximos aos múltiplos de q/r. Por outro lado, se r não divide q em partes iguais, então o resultado terá um comportamento aproximado, fazendo com que valores inteiros diferentes de zero estejam concentrados próximos aos múltiplos de q/r.

A *transformada rápida de Fourier* (FFT) é uma versão da DFT onde q é potência de dois. A *transformada quântica de Fourier* (QFT) é uma variante da transformada discreta de Fourier, e assim como a FFT, a quantidade de intervalos q é uma potência de dois. A QFT difere da FFT pelo fato da QFT ser projetada especialmente para os computadores quânticos. Isso significa que a QFT é dada em forma de matrizes de transformação e constituida de transformações unitárias. Além disso, a QFT é construída de forma que minimize o número de portas quânticas utilizadas.

A transformada quântica de Fourier (QFT) opera em funções, alterando as amplitudes do estado quântico. Isso significa que, ao manipular as amplitudes, a transformada conseqüentemente altera as probabilidades de medirmos certos estados numa sobreposição. Vamos denotar a aplicação da QFT como:

$$\sum_x g(x)|x\rangle \rightarrow \sum_c G(c)|c\rangle,$$

onde $G(c)$ é a função resultante após aplicada a transformada quântica de Fourier em $g(x)$ e tendo x e c na faixa de representação binária para os inteiros entre 0 e $q-1$. Se o estado é medido depois de aplicada a QFT, a probabilidade de observarmos o estado $|c\rangle$ será $||G(c)||^2$.

Ao aplicar a transformada quântica de Fourier na função periódica $g(x)$ (de período r), nós iremos obter o estado $\sum_c G(c)|c\rangle$, onde $G(c)$ é zero exceto nos múltiplos de q/r. Então, quando esse estado for medido, o resultado será um múltiplo de q/r, denotado por jq/r. Mas, como descrito acima, a transformada quântica de Fourier apenas dá resultados exatos para os períodos que são potências de 2, ou seja, períodos que dividem q (pois q também é potência de 2). Se o período não é potência de 2, então obteremos resultados aproximados, i.e., teremos alta probabilidade de medir resultados *próximos* a jq/r. Além disso, quanto maior o número de intervalos q utilizados na transformação, melhor a aproximação. A transformada quântica de Fourier U_{QFT} com base $q = 2^m$ é definido por

$$U_{QFT} : |x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi icx}{2^m}} |c\rangle.$$

A definição da transformação U_{QFT} descrita acima somente nos informa como essa transformada é implementada. Não precisamos entender o porquê

dessa transformação ser formulada assim. O principal objetivo com a QFT é entender a sua semântica: como ela vai modificar o estado quântico e porque ela é utilizada no algoritmo de Shor.

Em seu artigo de 1997, Shor estuda mais a fundo essa transformada, e constata que, para que o algoritmo de Shor seja um algoritmo polinomial, a transformada quântica de Fourier deve ser computacionalmente eficiente. Shor mostrou que a transformada quântica de Fourier com o número de intervalos igual a $q = 2^m$ pode ser construída utilizando apenas $(m(m+1))/2$ portas quânticas de 1 ou 2 qubits.

7.4 Passos do algoritmo de Shor

Abaixo vamos especificar detalhadamente cada passo do algoritmo de Shor, que fatora um dado inteiro N.

Passo 1 Se N é par, um dos fatores é 2, então rodamos o algoritmo de Shor novamente para fatorar $N/2$. Se N é primo, então não há necessidade de utilizar o algoritmo de Shor, e abortamos a execução. Para testar a primalidade de N, podemos utilizar o algoritmo AKS [31], que roda em tempo polinomial. Caso N seja uma potência de um número primo, também abortamos a execução do algoritmo. Existem métodos eficientes para testar se um dado número é uma potência de um número primo. O primeiro passo inteiro pode ser executado em um computador clássico.

Passo 2 Escolha aleatoriamente um inteiro x que seja co-primo a N. O algoritmo de Euclides é um método eficiente para testar se dois números são primos entre si. Se, após a execução do algoritmo de Euclides, x não é co-primo a N, então $\text{mdc}(x, N) \neq 1$ e deve-se escolher outro valor para x.

Passo 3 Escolha um inteiro $q = 2^m$ qualquer que é potência de dois, tal que $N^2 \leq q = 2^m \leq 2N^2$. O número q deve estar entre N^2 e $2N^2$ pois se, caso o período não for uma potência de 2, então a aproximação utilizada na QFT será suficientemente boa para que o algoritmo funcione.

Passo 4 Crie um registrador quântico e o divida em dois, registrador 1 e registrador 2. Assim o estado de nosso computador quântico pode ser dado por:

$$|\psi\rangle = |REG1\rangle|REG2\rangle.$$

O registrador 1 deve ter qubits suficientes para representar inteiros tão grandes quanto $q-1$ e o registrador 2 deve ter qubits suficientes para representar inteiros tão grandes quanto $N-1$. O cálculo da quantidade de qubits necessários pode ser realizado em um computador clássico.

Passo 5 Carregue o registrador 1 com uma sobreposição uniformemente distribuída (i.e.,todos os número com a mesma probabilidade de serem medidos) de todos os inteiros de 0 a $q-1$. Para configurarmos essa sobreposição, podemos utilizar a transformação Walsh-Hadamard. Carregue o registrador 2 com zeros. Esta operação deve ser feita pelo computador quântico. O estado do registrador neste ponto é:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0\rangle.$$

Passo 6 Agora aplique a transformação $x^a \mod N$ para cada número armazenado no registrador 1 e armazene o resultado no registrador 2. Devido ao paralelismo quântico, isto será executado em apenas um passo, porque o computador quântico calculará somente $x^{|a\rangle} \mod N$, onde $|a\rangle$ é a sobreposição dos estados criados no passo 5. Este passo é executado no computador quântico. O estado do registrador neste ponto é:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|x^a \mod N\rangle.$$

Passo 7 Realize uma medição no registrador 2. Seja k o valor resultante dessa medição. Note que, após a medição do registrador 2, o registrador 1 estará em uma sobreposição em função do que foi medido no registrador 2. Então, o registrador 1 conterá somente os valores x entre 0 e $q-1$ tal que

$$x^a \mod N = k.$$

Esta operação é executada pelo computador quântico. O estado do registrador depois deste passo é:

$$\frac{1}{\sqrt{|A|}}\sum_{a'\in A}|a'\rangle|k\rangle.$$

Onde A é o conjunto de a´s tal que $x^a \mod N = k$, e $|A|$ é o número de elementos nesse conjunto.

Passo 8 Agora deve-se aplicar a transformada quântica de Fourier no registrador 1. O registrador 2 não será mais utilizado, então, por questões de simplificação e clareza, não vamos mais escrevê-lo. A transformada quântica de Fourier quando aplicada ao estado $|a'\rangle$ muda o estado da seguinte maneira:

$$U_{QFT} : \frac{1}{\sqrt{|A|}} \sum_{a' \in X} |a'\rangle \rightarrow \sum_{c} G(c)|c\rangle.$$

Como afirmamos anteriormente, se o período r da função $x^a \mod N$ é uma potência de dois, então a função da tranformada de Fourier $\sum_c G(c)|c\rangle$ está definida como:

$$U_{QFT} : \sum_{c} G(c)|c\rangle = \sum_{j} c_j |jq/r\rangle.$$

Onde, $j(q/r)$ são os múltiplos de q/r. Então o estado atual do registrador está numa sobreposição onde todos os valores são múltiplos de q/r.

Passo 9 Realize uma medição no registrador 1. Seja v o valor resultante dessa medição. Se o período r for potência de dois, então v certamente é um múltiplo de q/r. Se r não for potência de dois, então v não é necessariamente um múltiplo de q/r, mas a probabilidade de que ele seja é alta.

Passo 10 Obtido o valor v, existem várias técnicas, executadas num computador clássico, que calculam o período r baseado no conhecimento do valor de v e q. Uma das técnicas mais utilizadas para isso é chamada de *método da expansão em frações contínuas*. Para explicar essa técnica clássica, reservamos a seção 7.5 deste capítulo.

Passo 11 Após obter r, se r é um número ímpar, então volte ao **Passo 1** para recomeçar o algoritmo escolhendo um x diferente do que havia sido escolhido. (**Obs**: as chances de r ser ímpar são de $1/2^z$, onde z é o número de fatores de N)

Passo 12 Um fator de N pode ser determinado pelo $\text{mdc}(x^{r/2}-1, N)$ e $\text{mdc}(x^{r/2}+1, N)$. Se você tiver encontrado um fator não-trivial de N então pare, senão volte ao passo 4. Fatores não-triviais são todos os fatores de N exceto 1 e o próprio N. Este passo final é realizado no computador clássico.

Os passos 11 e 12 contêm uma previsão sobre como proceder caso o algoritmo de Shor não produza fatores de N. Existem algumas poucas razões pela qual o algoritmo de Shor pode falhar:

- A transformada quântica de Fourier pode medir 0 no passo 9, fazendo que o processamento posterior no passo 10 seja impossível.
- O método da expansão em frações contínuas (Passo 10) pode não conseguir achar o período (ver seção 7.5).
- O período r pode ser ímpar, impossibilitando decompor $x^r - 1 \mod N$ em $(x^{r/2} - 1)(x^{r/2} + 1) \mod N$.
- O algoritmo irá algumas vezes encontrar os fatores 1 e N, os quais não são utilizáveis também.

O resultado do **Passo 7**, e conseqüentemente a aplicação da QFT no **Passo 8**, são melhores compreendidos apresentando um exemplo.

Seja $N = 21$ o número a ser fatorado, $x = 11$ co-primo a N. Assim, $f(a) = 11^a \mod 21$ é a função que é aplicada no registrador 2. Ao realizarmos a medição do registrador 2, obtemos a valor $k = 8$. Então, o conjunto X de valores que estarão em sobreposição no registrador 1 é dado por:

$$A = \{a | 11^a \mod 21 = 8\}.$$

Supondo que o intervalo está dividido igualmente em $q = 2^9 = 512$ partes, então o seguinte gráfico ilustra o estado atual do sistema:

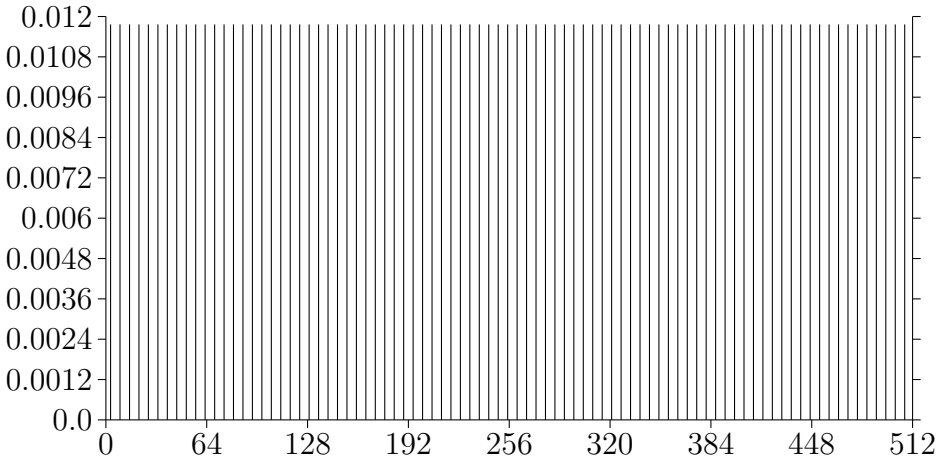


Figura 7.4.1: Probabilidade de obter a ao medir o estado $\sum_{a \in A} |a\rangle|8\rangle$, onde $A = \{a|11^a \mod 21 = 8\}$.

Após isso, seguimos ao **Passo 8**, onde será aplicada a QFT. Já adiantando, a função $f(a) = 11^a \mod 21$ tem período $r = 6$, mas esse período ainda nos é desconhecido. O gráfico abaixo representa a aplicação da QFT no estado atual do sistema:

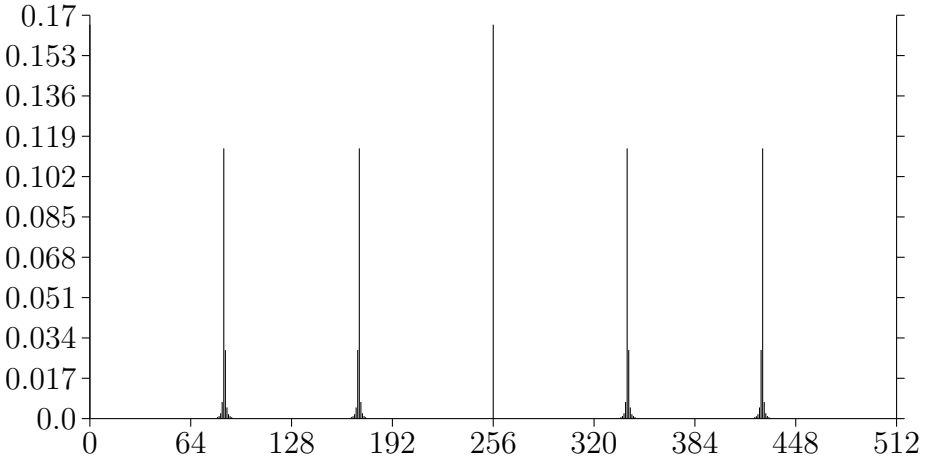


Figura 7.4.2: Distribuição de probabilidade após a aplicação da transformada quântica de Fourier.

Note que próximo ao valor $a = 85$, há probabilidades mais baixas de medir valores próximos como, por exemplo, 84 e 86. Isso é devido ao período r não ser uma potência de 2. Essa "não-exatidão" não provoca impactos muito significativos, pois a probabilidade de medir os resultados aproximados é baixa.

Então, temos 7 principais picos de probabilidades que podem ser medidos: $\{0, 85, 171, 256, 341, 427, 512\}$. Desconsiderando as baixas probabilidades de medirmos os resultados aproximados, o estado do sistema é:

$$\sqrt{0.17}|0\rangle + \sqrt{0.12}|85\rangle + \sqrt{0.12}|171\rangle + \sqrt{0.17}|256\rangle + \\ \sqrt{0.12}|341\rangle + \sqrt{0.12}|427\rangle + \sqrt{0.17}|512\rangle$$

Note que os valores $0, 85, 171, 256, 341, 427, 512$ são todos múltiplos aproximados de q/r.

Agora, ao realizarmos uma medição no estado atual, suponha que obtivemos o valor $v = 427$. Então devemos calcular o valor do período utilizando, por exemplo, o método da expansão em frações contínuas, que será explicado na Seção 7.5. Existem outro métodos que, dados v e q, encontram o período r da função.

Assim, após utilizar o método, descobrimos que $r = 6$. Tivemos sorte de conseguirmos um período par. Então podemos calcular os fatores de $N = 21$. Sabemos que

$$x^{6/2} - 1 = 11^3 - 1 = 1330$$

ou

$$x^{6/2} + 1 = 11^3 + 1 = 1332$$

têm um fator comum com $N = 21$. Ao executar o algoritmo de Euclides, obtemos $\text{mdc}(21, 1330) = 7$ e $\text{mdc}(21, 1332) = 3$. Nesse problema em particular, obtivemos dois fatores, o que não ocorre comumente. Na maioria das vezes, conseguimos somente um fator a cada execução. Em algumas poucas vezes, não obtemos nenhum fator, então devemos executar novamente o algoritmo.

7.5 Expansão em frações contínuas: encontrando o período

Na maioria dos casos, o período r não divide 2^m, e o valor v medido no passo 9 do algoritmo de Shor possui alta probabilidade de ser um valor próximo a um múltiplo de $\frac{2^m}{r}$, ou seja, próximo a $j\frac{2^m}{r}$ para algum $j \in \mathbb{N}$.

Para extrair o valor r do valor medido v, usamos a sequência das seguintes equações[2]:

$$
\begin{aligned}
a_0 &= \left\lfloor \frac{v}{2^m} \right\rfloor, \\
\epsilon_0 &= \frac{v}{2^m} - a_0, \\
a_n &= \left\lfloor \frac{1}{\epsilon_{n-1}} \right\rfloor, \\
\epsilon_n &= \frac{1}{\epsilon_{n-1}} - a_n, \\
p_0 &= a_0, \\
p_1 &= a_1 a_0 + 1, \\
p_n &= a_n p_{n-1} + p_{n-2}, \\
q_0 &= 1, \\
q_1 &= a_1, \\
q_n &= a_n q_{n-1} + q_{n-2}.
\end{aligned}
$$

Seja $f(a) = x^a \mod N$ a função que estamos utilizando no algoritmo de Shor. Então, há duas condições de parada para esse método. Devemos parar se:

- $x^{q_i} \mod N = 1$, onde q_i é o valor de q na i-ésima iteração. Existem métodos eficientes (de tempo polinomial) para testar essa condição. Nesse caso, obtivemos o período $r = q_i$ com **sucesso**.

- $q_i \geq N$, pois, como q_i é o suposto período, é impossível a função ter período maior que N. Nesse caso, o método **não obteve sucesso** encontrando o período.

Caso paremos pela primeira condição, então tivemos sucesso e utilizamos o valor q_i obtido pelo método como sendo o período r.

Exemplo: Suponha que o valor a ser fatorado é 21, sabemos que $q = 512$ e foi medido $v = 427$. Então v e $2^m = q$ são relativamente primos, o período r não divide 2^m e a expansão das frações tem de ser aplicada.

[2]Não confundir a variável q_i do algoritmo da expansão de frações contínuas com a variável $q = 2^m$ (número pontos igualmente distribuidos da QFT) do algoritmo de Shor.

i	a_i	p_i	q_i	ϵ_i
0	0	0	1	0.8339844
1	1	1	1	0.1990632
2	5	5	6	0.02352941
3	42	211	253	0.5

o qual termina com 6, onde $q_2 < N \leq q_3$. Então $r = 6$ é o período da função f.

Impossibilidade de solução

Como demonstramos no exemplo da Figura 7.4.2, o método descrito acima funcionou para o valor $v = 427$, no entanto, se medíssemos qualquer outro dos possíveis valores (0, 85, 171, 256, 341 ou 512) este método iria falhar e não nos retornaria o período r. Isso se deve ao fato de que esse método só funciona quando o fator multiplicativo j é co-primo ao período r. Podemos reescrever os valores possíveis da seguinte maneira:

$$\begin{aligned} 0 &= 0 * q/r, \\ 85 &= 1 * q/r, \\ 171 &= 2 * q/r, \\ 256 &= 3 * q/r, \\ 341 &= 4 * q/r, \\ 427 &= 5 * q/r, \\ 512 &= 6 * q/r. \end{aligned}$$

O fator multiplicativo j varia entre 0 e 6. O único valor de j que é co-primo ao valor de r (sabendo antecipadamente que $r = 6$) é $j = 5$. Os outros j's (0,1,2,3,4,6) não são co-primos a r. Por isso, nesse exemplo, o método só funciona para $v = 427$, que é onde $j = 5$.

Caso tenhamos medido algum valor v que impossibilite o cálculo do período, devemos executar novamente o algoritmo. Estudos [24, 21] mostram que se deve executar $O(\log \log r)$ vezes o algoritmo para que tenhamos probabilidade alta de conseguir achar o período através deste método.

O método da expansão de frações contínuas é executado em tempo polinomial no tamanho das entradas. Como, em média, devemos executar o método $O(\log \log r)$ vezes, então $O(\log \log r) \times$tempo polinomial $\in$ P. Em outras palavras, mesmo executando várias vezes este método, o algoritmo de Shor continua rodando em tempo polinomial.

Mais resultados sobre este método podem ser encontrados em [21].

7.6 Um caso especial

Vamos agora mostrar passo-a-passo como $N = 91$ $(= 7 \cdot 13)$ pode ser fatorado usando o algoritmo de Shor.

Passo 1 O número $N = 91$ não é par, não é primo e não é potência de um primo. Então podemos executar o algoritmo de Shor.

Passo 2 Aleatoriamente, escolhemos um inteiro positivo $x = 3$. Como $\text{mdc}(91, 3) = 1$, então vamos continuar a execução e tentar encontrar o período da função f, onde f é dada por

$$f(a) = 3^a \mod 91.$$

A função f tem período $r = 6$, mas esse valor é desconhecido por nós. A tabela abaixo mostra alguns valores da função $f(a)$,

a	0	1	2	3	4	5	6	7	$\cdots$
$f(a)$	1	3	9	27	81	61	1	3	$\cdots$
$\therefore$ Período a ser descoberto: $r = 6$									

Passo 3 Escolhemos $q = 2^{14} = 16384$ tal que $N^2 \leq q < 2N^2$.

Passo 4 Inicializar os registradores 1 e 2. Então, o estado dos dois registradores fica:

$$|\psi\rangle = |0\rangle\,|0\rangle\,.$$

O registrador 1 tem 14 bits, enquanto que o registrador 2 tem 7 bits.

Passo 5 Ao executar a transformada Walsh-Hadamard no registrador 1, obtemos:

$$\frac{1}{\sqrt{16384}} \sum_{a=0}^{16383} |a\rangle|0\rangle.$$

Passo 6 Aplicando a tranformação unitária $f(a) = 3^a \mod 91$ no registrador 2, temos:

$$\frac{1}{\sqrt{16384}} \sum_{a=0}^{16383} |a\rangle|3^a \mod 91\rangle$$

Então, o estado dos registradores fica:

$$\begin{aligned}
&\tfrac{1}{\sqrt{16384}} \ \sum_{a=0}^{16383} |a\rangle\,|3^a \mod 91\rangle \\
= \ &\tfrac{1}{\sqrt{16384}}(\quad |\,0\rangle\,|1\rangle \ + |\,1\rangle\,|3\rangle + |\,2\rangle\,|9\rangle \ + |\,3\rangle\,|27\rangle + |\,4\rangle\,|81\rangle + |\,5\rangle\,|61\rangle \\
&+ \ |\,6\rangle\,|1\rangle \ + |\,7\rangle\,|3\rangle + |\,8\rangle\,|9\rangle \ + |\,9\rangle\,|27\rangle + |10\rangle\,|81\rangle + |11\rangle\,|61\rangle \\
&+ \ |12\rangle\,|1\rangle \ + |13\rangle\,|3\rangle \ + |14\rangle\,|9\rangle \ + |15\rangle\,|27\rangle + |16\rangle\,|81\rangle + |17\rangle\,|61\rangle \\
&+ \ \ldots \\
&+ \ |16380\rangle\,|1\rangle + |16381\rangle\,|3\rangle + |16382\rangle\,|9\rangle + |16383\rangle\,|27\rangle \\
&)
\end{aligned}$$

O estado dos dois registradores é mais do que uma sobreposição de estados. Após o passo acima, temos um estado quântico emaranhado dos dois registradores.

Passo 7 Ao medirmos o registrador 2, obtemos o valor $k = 3$. Então teremos:

$$\frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a'\rangle|3\rangle, \ \text{onde} |A| = 2731.$$

Então, o estado dos registradores fica:

$$\begin{aligned}
&\tfrac{1}{\sqrt{2731}} \ \sum_{a' \in A} |a'\rangle\,|3\rangle \\
= \ &\tfrac{1}{\sqrt{2731}}(\quad |\,1\rangle\,|3\rangle \ + |\,7\rangle\,|3\rangle + |\,13\rangle\,|3\rangle \ + |\,19\rangle\,|3\rangle + |\,25\rangle\,|3\rangle + |\,31\rangle\,|3\rangle \\
&+ \ |\,37\rangle\,|3\rangle \ + |\,43\rangle\,|3\rangle + |\,49\rangle\,|3\rangle \ + |\,55\rangle\,|3\rangle + |61\rangle\,|3\rangle + |67\rangle\,|3\rangle \\
&+ \ |73\rangle\,|3\rangle \ + |79\rangle\,|3\rangle \ + |85\rangle\,|3\rangle \ + |91\rangle\,|3\rangle + |97\rangle\,|3\rangle + |103\rangle\,|3\rangle \\
&+ \ \ldots \\
&+ \ |16363\rangle\,|3\rangle + |16369\rangle\,|3\rangle + |16375\rangle\,|3\rangle + |16381\rangle\,|3\rangle \\
&).
\end{aligned}$$

Passo 8 O próximo passo é aplicar a transformada quântica de Fourier no registrador 1. Como o período não é uma potência de 2, teremos resultados

aproximados que poderão ser medidos com uma probabilidade muito baixa. No entanto, por questões de exemplificação, vamos desconsiderar tais resultados aproximados. Então o estado dos registradores fica:

$$\begin{aligned} & \tfrac{1}{\sqrt{7}} \ \sum_{c\in G} |c\rangle\,|3\rangle \\ = \ & \tfrac{1}{\sqrt{7}}(\quad |0\rangle\,|3\rangle + \ |\ 2731\rangle\,|3\rangle + \ |\ 5461\rangle\,|3\rangle + \ |\ 8192\rangle\,|3\rangle \\ & \quad + \ |\ 10923\rangle\,|3\rangle + \ |\ 13653\rangle\,|3\rangle + \ |\ 16384\rangle\,|3\rangle \\ & \ ). \end{aligned}$$

Passo 9 Ao medir o registrador 1, obtemos o valor $v = 13653$.

Passo 10 Tendo $v = 13653$ e $q = 16384$, vamos computar o valor do período utilizando o **método da expansão em frações contínuas**, explicado na Seção 7.5.

i	a_i	p_i	q_i	ϵ_i
0	0	0	1	0.833312988
1	1	1	1	0.200029298
2	4	4	5	0.999267657
3	1	5	6	0.00073288
4	1364	6824	8189	0.47986

o qual termina com 6, pois $x^{q_3} = 3^6 \text{mod} 91 = 1$ onde $q_3 < N \leq q_4$. Então $r = 6$ é o período procurado.

Passo 11 O período $r = 6$ é um número par, portanto podemos ir para o próximo passo.

Passo 12 Utilizando o algoritmo de Euclides, calculamos $\text{mdc}(3^{6/2} - 1, 91)$ e $\text{mdc}(3^{6/2} + 1, 91)$, onde:

$$\text{mdc}(3^{6/2} - 1, 91) = \text{mdc}(26, 91) = 13$$

e

$$\text{mdc}(3^{6/2} + 1, 91) = \text{mdc}(28, 91) = 7$$

Assim, encontramos os números 7 e 13, e ambos são fatores de $N = 91$.

Capítulo 8

Algoritmo de Grover

Problemas de busca em computação se resumem em como encontrar um elemento em um conjunto de dados. Um problema de busca pode ser especificado como um problema onde um predicado $P(x)$ é verdadeiro para o elemento x procurado.

Uma busca estruturada é uma busca onde há informações sobre a estrutura do espaço de busca, como por exemplo, um conjunto de dados em ordem alfabética. Nesse caso é possível explorar essa estrutura para construir algoritmos eficientes. Em outros casos a estrutura do problema pode ser utilizada para criar algoritmos baseados em heurísticas que resultam em soluções eficientes para algumas instâncias do problema.

Um conjunto de dados não estruturado significa que não se sabe nada a respeito de como os dados estão organizados. Em um problema de busca nesse tipo de conjunto de dados, ou busca não estruturada, nada é assumido em relação à estrutura do espaço de soluções.

Suponha um grande conjunto de dados não estruturado de tamanho N. Ao realizarmos uma busca nesse conjunto de dados, a única maneira de encontrarmos um elemento é pesquisando um a um, ou seja, é necessário executar uma busca linear. Se tentarmos encontrar um elemento marcado[1] nesse conjunto de dados que contém N elementos examinando apenas K elementos, temos a probabilidade $\frac{K}{N}Q$ de encontrar o elemento que procuramos, onde Q é a probabilidade de o elemento procurado estar presente no conjunto. Então é necessário examinar N elementos para termos uma probabilidade Q de encontrarmos o elemento marcado.

Uma busca com sucesso em um conjunto onde os dados estão distribuídos aleatoriamente necessita, em média, de $\frac{N+1}{2}$ comparações. O melhor caso é

[1] Ao aplicarmos uma função a um elemento marcado, a função retorna um valor diferente de todos os outros elementos do conjunto. Por exemplo, o valor 1 é retornado pela função para o elemento marcado, o o valor 0 é retornado para todos os outros elementos.

quando o elemento procurado está na primeira posição (1 comparação). O pior caso é o contrário, quando o elemento procurado está na ultima posição (N comparações). Se N é muito grande, então o algoritmo de Grover proporciona um aumento significativo no desempenho em buscas não estruturadas.

O algoritmo de Grover é freqüentemente dito ser um algoritmo de busca, mas o que este algoritmo realmente faz é inversão de funções. Se uma função $f(x) = y$ pode ser computada em um computador quântico, então esse algoritmo pode calcular x , dado y. Como todo algoritmo quântico, o algoritmo de Grover é probabilístico, ou seja, retorna a resposta correta com alta probabilidade.

Este algoritmo proporciona uma melhora quadrática no desempenho em comparação ao algoritmo clássico de busca, diferentemente de outros algoritmos quânticos, que proporcionam melhoras exponenciais em relação a seus similares clássicos. A complexidade do algoritmo de Grover é $O(\sqrt{N})$.

Grover ainda propôs um outro algoritmo para busca, este em dados estruturados, que utiliza o algoritmo que veremos nesta seção. Grover [37] usa o algoritmo de busca de Grover em conjunto com um algoritmo de heurísticas para solucionar problemas NP-difícil, obtendo ganho quadrático de desempenho em relação aos algoritmos clássicos. [14] mostrou que algoritmos heurísticos gerais de busca têm algoritmos quânticos análogos com aumento de desempenho quadrático. O algoritmo de Grover pode ser utilizado para resolver problemas NP-completos com procuras exaustivas por todo o espaço de soluções. Isto resulta em um ganho de desempenho considerável em relação aos algoritmos clássicos, mas não alcança tempo polinomial para problemas NP-completos.

Em seu artigo [20], Grover aborda apenas buscas por um único item. Em aplicações práticas, várias vezes nos deparamos com buscas onde mais de um item satisfazem o critério utilizado na busca. Na mais simples generalização do algoritmo de Grover, o número de itens que satisfazem o critério de busca deve ser conhecido. Essa generalização foi apresentada por Choong Chen, Stephen A. Fulling e Marlan O. Scully [15].

8.1 Operadores utilizados no algoritmo

8.1.1 Operador para rotacionar fase

A matriz que representa uma rotação de fase tem a forma de uma matriz diagonal, com $R_{kc} = 0$ se $k \neq c$, e $R_{kk} = e^{i\phi_k}$, onde ϕ_k é um número real

arbitrário e $i = \sqrt{-1}$. Para um sistema onde $n = 4$, a matriz seria:

$$\mathbf{R} = \begin{pmatrix} e^{i\phi_1} & 0 & 0 & 0 \\ 0 & e^{i\phi_2} & 0 & 0 \\ 0 & 0 & e^{i\phi_3} & 0 \\ 0 & 0 & 0 & e^{i\phi_4} \end{pmatrix}.$$

Da fórmula de Euler,

$$e^{ix} = \cos x + i \sin x,$$

$$e^{-ix} = \cos x - i \sin x,$$

extraímos que as entradas diagonais são equivalentes a $\cos \phi_k + i \sin \phi_k$.

Para o algoritmo de Grover precisamos de uma rotação seletiva de fase, ou seja, precisamos de uma matriz que rotacione em π radianos apenas a fase do estado marcado. Esta matriz será uma matriz diagonal com $1's$ em toda a diagonal, exceto no K-ésimo elemento da diagonal, que será -1, quando o estado marcado é o estado K. Obviamente, não podemos construir nada parecido com esse operador classicamente, sendo que para isso precisariamos saber qual é o estado marcado anteriormente. Como uma porta como esta pode ser implementada na mecânica quântica é um tanto obscuro. Em uma implementação prática, o sistema quântico deveria "sentir" o estado, e então, dependendo da resposta, rotacionar ou não a fase. Isto deve ser feito de uma maneira que não deixe rastros após a medição, pois o resultado final deve ser *somente* rotacionar a fase do estado desejado.

8.1.2 Operador para criar sobreposição igual de estados

Já vimos que uma sobreposição igual de estados é criada utilizando o operador Walsh-Hadamard. Um bit no estado 0 é transformado para uma sobreposição de dois estados: $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$. Da mesma maneira, um bit no estado 1 é transformado para $(\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}})$. Isso significa que a magnitude em cada estado é a mesma, $\frac{1}{\sqrt{2}}$, mas a fase da amplitude no estado 1 fica invertida.

Esta operação pode ser feita em tempo $O(n) = O(\log N)$. Para simulá-la em um computador clássico, precisamos realizar $O(N)$ operações. Este é um exemplo do ganho exponencial na simulação clássica de sistemas quânticos, observado por Feynman.

8.1.3 Operador de inversão sobre a média

A inversão sobre a média no vetor de estados é um operador que aumenta ou diminui a amplitude de um estado. A amplitude é aumentada o quanto o estado estava abaixo da média, ou diminuída o quanto e estado estava acima da média antes da operação.

Para efetuar esta operação em um computador quântico, esta deve ser uma transformação unitária. Além disso, para que o algoritmo todo resolva o problema em tempo $O(\sqrt{N})$, a inversão deve ser feita de forma eficiente. A operação de inversão pode ser feita em $O(n) = O(\log N)$ portas quânticas.

A transformação

$$\sum_{i=0}^{N-1} a_i|x_i\rangle \quad \rightarrow \quad \sum_{i=0}^{N-1} 2A - a_i|x_i\rangle,$$

onde A é a média dos a_i's, é realizada pela matriz $N \times N$:

$$\mathbf{D} = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1 \end{pmatrix}.$$

Como $DD^* = I$, D é unitária e conseqüentemente é uma possível transformação quântica.

De acordo com Grover, D pode ser definido como $D = WRW$, onde W é a transformação de Walsh-Hadamard e

$$\mathbf{R} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots \\ 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Para mostrarmos que $D = WRW$, considere $R = R' - I$, onde I é a matriz identidade e

$$\mathbf{R}' = \begin{pmatrix} 2 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots \\ 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}.$$

Agora $WRW = W(R' - I)W = WR'W - I$. Então

$$\mathbf{WR'W} = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix}.$$

Deste modo $WR'W - I = D$.

8.1.4 Inversão de sinal

Seja U_P, tal que $U_P : |x, b\rangle \rightarrow |x, b \oplus P(x)\rangle$, onde $\oplus$ é o operador OR exclusivo. Aplicando U_p à sobreposição $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} |x\rangle$ e escolhendo $b = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ para terminar em um estado onde o sinal de todos os x com $P(x) = 1$ sejam invertidos e b não seja alterado. Seja $X_0 = \{x \mid P(x) = 0\}$ e $X_1 = \{x \mid P(x) = 1\}$. Aplicando U_P:

$$\begin{aligned} & U_P(|\psi, b\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} U_P(\sum_{x \in X_0} |x, 0\rangle + \sum_{x \in X_1} |x, 0\rangle - \sum_{x \in X_0} |x, 1\rangle - \sum_{x \in X_1} |x, 1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}}(\sum_{x \in X_0} |x, 0 \oplus 0\rangle + \sum_{x \in X_1} |x, 0 \oplus 1\rangle - \sum_{x \in X_0} |x, 1 \oplus 0\rangle - \sum_{x \in X_1} |x, 1 \oplus 1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}}(\sum_{x \in X_0} |x, 0\rangle + \sum_{x \in X_1} |x, 1\rangle - \sum_{x \in X_0} |x, 1\rangle - \sum_{x \in X_1} |x, 0\rangle) \\ &= \frac{1}{\sqrt{2^{n}}}(\sum_{x \in X_0} |x\rangle - \sum_{x \in X_1} |x\rangle) \otimes b. \end{aligned}$$

Desse modo as amplitudes dos estados em X_1 foram invertidas.

8.2 Passos do algoritmo de Grover

Para entendermos o algoritmo de Grover, vamos assumir o seguinte:

- Um sistema com $N = 2^n$ estados rotulados $S_1, S_2, ..., S_N$.
- Estados representados por strings de n bits.

- Um único elemento marcado S_m que satisfaz $C(S_m) = 1$.
- Para todos os outros estados, $C(S) = 0$.
- C pode ser executado em uma unidade de tempo.

1. O primeiro passo do algoritmo de Grover é colocar o registrador em uma sobreposição igual de todos os estados: $(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, ..., \frac{1}{\sqrt{N}})$, aplicando o operador de Walsh-Hadamard W.

2. Repita[2] $O(\sqrt{N})$ vezes os passos a e b:

   a. Estando o sistema em um estado S, se $C(S) = 1$ então rotacione a fase em π radianos. Senão mantenha o sistema inalterado. Note que esta operação não tem análoga clássica. Nós não observamos o estado do registrador, pois se isso fosse feito iria colapsar a sobreposição de estados para um estado do sistema. A porta de rotação de fase seletiva seria um operador da mecânica quântica que rotacionaria somente a amplitude do estado marcado dentro da sobreposição.

   b. Aplique sobre o registrador o operador de inversão sobre a média A , cuja matriz é

$$A_{kc} = \frac{2}{N},\ k \neq c$$

$$A_{kk} \ = \ -1 + \frac{2}{N}$$

3. Faça a medição do registrador quântico. A medição resultará no rótulo de n bits do estado marcado $C(S_m) = 1$ com probabilidade no mínimo $0,5$. [20]

Uma questão em aberto nesse algoritmo acima é quantas vezes o passo 2 deve ser repetido. Grover provou a existência de um $m \in O(\sqrt{N})$ tal que após m iterações do passo 2 do algoritmo, a probabilidade de encontrar o registrador no estado marcado é no mínimo 0,5. Boyer [34] faz uma análise

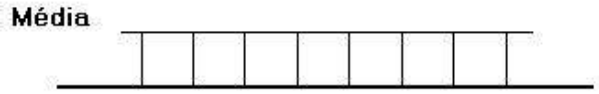
[2] O número preciso de iterações é importante e será explicado adiante.

detalhada da performance do algoritmo de Grover, provando que é um algoritmo ótimo (nenhum algoritmo pode fazer uma busca não estruturada de maneira mais rápida). Além disso, também mostra que se há somente um S_0 onde $C(S_0) = 1$, então após $\frac{\pi}{8\sqrt{2^n}}$ iterações do passo dois, a taxa de erro é de $0,5$, que é a taxa citada por Grover em seu algoritmo. Após $\frac{\pi}{4\sqrt{2^n}}$ iterações, a taxa de erro cai para 2^{-n}. Iterações adicionais aumentam a taxa de erro. Por exemplo, após $\frac{\pi}{2\sqrt{2^n}}$ iterações, a taxa de erro se aproxima de 1.

8.2.1 Ilustração do algoritmo de Grover

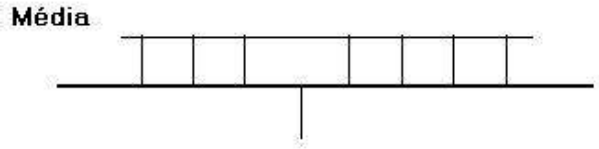
Os gráficos a seguir mostram como funciona o algoritmo de Grover em um registrador de 3 bits.

Efetuamos a transformação de Walsh-Hadamard, deixando o registrador em uma sobreposição igual dos oito estados possíveis.



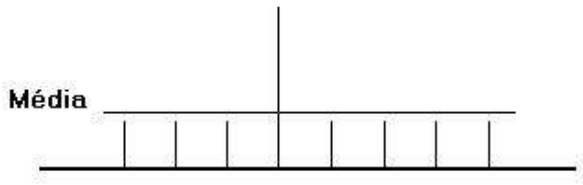
Registrador após Walsh-Hadamard.

Então efetuamos a inversão de fase seletiva, que inverte o sinal da amplitude do estado marcado. Neste gráfico, o estado marcado é o estado 4.



Registrador após inversão de fase seletiva.

Finalmente efetuamos o operador de inversão sobre a média, que aumenta a amplitude do estado desejado, que foi invertido na operação anterior.



Registrador após inversão sobre a média.

8.3 Um caso especial

No caso especial onde $N = 4$, o número preciso de iterações necessárias para se fazer a leitura correta do resultado é 1. Com este caso especial, podemos ver de forma melhor como o algoritmo de Grover explora a interferência entre os estados para aumentar a amplitude do estado desejado.

Para um sistema quântico onde $N = 4$, temos as seguites matrizes para efetuar as operações necessárias:

$$\mathbf{W} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$\mathbf{A} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Seja (a, b, c, d) o vetor de amplitudes, onde a^2 é a probabilidade de medir o estado 00, b^2 a probabilidade de medir o estado 01, c^2 a probabilidade de medir o estado 10 e d^2 a probabilidade de medir o estado 11.

Vamos supor que o elemento marcado é o terceiro. Em um sistema com $N = 4$, o algoritmo de Grover se resume a:

1) Registrador quântico no estado 00 com probabilidade 1 : $REG = (1, 0, 0, 0)^T$

2) Aplicar W em REG.
Após este passo, temos o registrador no estado $W * (1, 0, 0, 0)^T = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})^T$.

3) Se $C(REG) = 1$, fazer a inversão de fase.
Ao fim deste passo, teremos o estado $(\frac{1}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{1}{2})$, pois o elemento marcado é o terceiro, e este sofre a inversão de sinal.

4) Aplicar A em REG.
Após este passo, teremos nosso registrador no estado $A * (\frac{1}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{1}{2}) = (0, 0, 1, 0)^T$.

5) Fazer a leitura do estado de REG.

No quinto passo, como o registrador está no estado $(0, 0, 1, 0)^T$, teremos a medição do terceiro estado com probabilidade 1.

Entretanto, esse é um caso especial e em geral a probabilidade 1 não é atingida com nenhum número exato de iterações.

Capítulo 9

Complexidade Quântica

O objetivo dessa seção é mostrar alguns resultados da complexidade quântica baseado nos aspectos vistos até agora. Muitos resultados já foram conseguidos na teoria da complexidade quântica, no entanto, somente alguns desses resultados serão enunciados, e nenhum deles será provado, fazendo com que essa seção adquira um caráter mais informativo que explicativo, a fim de ilustrar as principais diferenças entre a computação clássica e a computação quântica. Várias fontes bibliográficas tratam desse assunto mais a fundo, e o leitor interessado deve recorrer a essas fontes (ver [10, 38, 17, 16]).

9.1 Definições Iniciais

Antes de apresentarmos os resultados da teoria da complexidade quântica, iremos estabelecer algumas definições que ajudarão a compreensão de tais resultados. Todas essas definições são explicadas de modo informal.

Definição 9.1.1. *Uma **MT probabilística** é uma máquina equivalente à MT a não ser pelo fato de podermos escolher aleatoriamente um caminho da execução.*

Na MT probabilística, por exemplo, ao realizarmos uma escrita na fita, o valor escrito é aleatório, igualmente distribuído entre 0 e 1. A MT não-determinística funciona como a MT probabilística, a não ser pelo fato que a MT não-determinística sempre adivinha a resposta correta (se ela existir). Assim sendo, podemos observar que a MT probabilística fornece resultados probabilísticos, ou seja, a resposta pode ou não estar correta, de acordo com uma certa probabilidade.

Definição 9.1.1. *A **classe BPP**("Bounded-error Probabilistic Polynomial time") é a classe dos problemas que são resolvidos por uma MT probabilística em tempo polinomial.*

Os problemas da classe BPP têm probabilidade de erro ε, ou seja, apresentarem a resposta errada com probabilidade ε.

Definição 9.1.1. *A **classe QP**("Quantum Polynomial time") é a classe dos problemas que são resolvidos por um Computador Quântico determinístico*[1] *em tempo polinomial.*

Essa classe não têm probabilidade de erro, pois, como os problemas são executados num computador quântico que não utiliza estados sobrepostos, então não há medições probabilísticas dos estados quânticos.

Definição 9.1.1. *A **classe BQP**("Bounded-error Quantum Polynomial") é a classe dos problemas que são resolvidos por um Computador Quântico probabilístico em tempo polinomial.*

Os problemas da classe BQP podem apresentar a resposta errada com probabilidade ε. Isso porquem, no computador quântico probabilístico, utiliza-se estados sobrepostos, possibilitando medições probabilísticas dos estados quânticos. A classe BQP é o análogo quântico da classe BPP.

9.2 P $\subseteq$ QP e BPP $\subseteq$ BQP

Um importante resultado da teoria da álgebra Booleana é que qualquer função Booleana pode ser escrita como composição das portas AND e NOT, e por isso elas são chamadas de *conjunto universal* de portas. Diferentemente da abordagem clássica de circuitos, os circuitos quânticos não têm um conjunto "base" de portas lógicas (como $\wedge$, $\vee$ e $\neg$) as quais os outros circuitos são derivados. O número de portas quânticas possíveis é infinito, uma vez que as portas quânticas são na verdade matrizes de números complexos. Mesmo restringindo o tamanho das portas a 1, 2 ou 3 qubits (ou, analogamente, matrizes de tamanho 2×2, $2^2 \times 2^2$ e $2^3 \times 2^3$) ainda assim existem infinitas portas quânticas possíveis. No entanto há algumas portas convencionais que são geralmente utilizadas e que servem como base para construir circuitos quânticos mais complexos. O conjunto dessas portas convencionais é chamada de *conjunto universal de portas quânticas.* Então segue o teorema:

[1] A definição correta para "Computador Quântico" seria "MT quântica", no entanto, por razões de comentadas anteriormente nesse documento, achou-se inconveniente apresentar o conceito de MT quântica.

Teorema 9.2.1. *Qualquer porta quântica de múltiplos qubits pode ser construida a partir de portas C-NOT e portas quântica simples (1 qubit).*

Esse é um dos mais importantes resultados sobre portas quânticas, pois não é conhecida a existência de um conjunto universal de portas clássicas reversíveis de 2 bits.

Como visto anteriormente, conseguimos criar portas quânticas reversíveis que têm a mesma funcionalidade de algumas portas clássicas irreversíveis. A porta de Toffoli consegue simular um AND clássico. Além disso, construímos o NOT quântico, que aplicado a estados quânticos base (i.e, estados que não estão em sobreposição) possui a mesma tabela-verdade do NOT clássico. Assim, com somente essas duas operações em um computador quântico, podemos simular qualquer computação clássica, pois, como dito acima, o AND e NOT clássicos conseguem simular qualquer função Booleana.

Um resultado importante da teoria da complexidade computacional é que a avaliação de funções reversíveis é tão boa quanto a avaliação de funções irreversíveis. Isso significa que se uma dada função irreversível pode ser computada em tempo polinomial, então ela também pode ser computada em tempo polinomial usando computação reversível. Esse resultado, juntamente com o fato de que um computador quântico consegue simular as portas clássicas AND e NOT (portanto consegue simular qualquer função booleana) prova que um computador quântico pode simular um computador clássico com uma diferença de ordem polinomial. Na verdade, converter um circuito irreversível para um reversível aumenta o tamanho do circuito por um fator constante, então

$$P = revP,$$

onde $revP$ é a classe de problemas que podem ser resolvidos em tempo polinomial reversívelmente. Além disso, como vimos que um computador quântico pode simular um computador clássico com uma sobrecarga de tempo polinomial, então

$$P \subseteq QP.$$

Se tivermos um registrador de n qubits inicialmente configurados em 0, e depois aplicarmos a transformação Walsh-Hadamard, ao realizarmos uma medição, vamos obter n bits aleatoriamente, uniformemente distribuidos. Como é simples gerar informação aleatória num computador quântico, e como $P \subseteq QP$, então temos

$$BPP \subseteq BQP.$$

A computação quântica ganhou fama por apresentar fortes argumentos de que há problemas que estão em BQP mas não estão em P. Os problemas

que ainda não foram descobertos estarem em P, mas estão em BQP são os seguintes:

- Fatoração de inteiros (algoritmo de Shor);
- Logaritmos discretos;
- Simulação de sistemas quânticos (computador quântico universal).

Antes de prosseguirmos, vamos fazer algumas definições.

Seja P um problema, $x \in I$ são as instâncias desse problema e $S(x)$ um conjunto finito de soluções para a instância x. Por exemplo, se P é o problema dos circuitos hamiltonianos, então o conjunto I consiste de todos os grafos finitos e para cada grafo $x \in I$, o conjunto $S(x)$ é constituído de todos os circuitos hamiltonianos do grafo x. P é chamado de *problema de enumeração*, ou seja, um problema de enumeração consiste em contarmos quantas soluções um problema tem. No caso do circuito hamiltoniano, o problema é saber quantos circuitos hamiltonianos um grafo tem.

Definição 9.2.1. *Um dado problema pertence à classe $\#\boldsymbol{P}$ se esse problema computa f, onde f é uma função que fornece a cardinalidade do conjunto dos caminhos aceitos por uma MT não-determinística.*

Definição 9.2.1. *Seja f uma problema que pertence a $\#P$. Seja M uma máquina de Turing com um oráculo que resolve f em passo unitário. Então a classe $\boldsymbol{P}^{\#P}$ é a classe dos problemas que são resolvidos em tempo polinomial pela máquina M.*

Agora podemos enunciar os próximos resultados obtidos na teoria da complexidade quântica.

O melhor limite superior conhecido para a classe BQP é $BQP \subseteq P^{\#P} \subseteq PSPACE$, isto é, todo problema que é resolvido em tempo polinomial numa Máquina de Turing quântica pode também ser resolvido usando quantidade polinomial de espaço na memória na Máquina de Turing Clássica. Portanto $P \subseteq BPP \subseteq BQP \subseteq P^{\#P} \subseteq PSPACE$. Uma vez que $P \stackrel{?}{=} PSPACE$ é uma grande questão aberta na teoria da complexidade computacional, isso implica que qualquer resultado absoluto mostrando que computadores quânticos são mais poderosos que computadores clássicos ($BQP \neq BPP$) terá que esperar uma por uma grande descoberta na teoria da complexidade. Por enquanto, temos de nos satisfazer com as evidências de que os computadores quânticos violam a tese atual de Church-Turing.

9.3 NP ⊆ BQP?

NP ⊆ BQP? Do ponto de vista do aumento exponencial de velocidade oferecido por computadores quânticos para certos problemas computacionais, é natural perguntar se computadores quânticos podem resolver problemas NP-completo em tempo polinomial. Uma resposta afirmativa teria consequências gigantescas, uma vez que os problemas NP-completo inclui milhares dos mais importantes problemas computacionais, e que são tidos como intratáveis classicamente. Pesquisas mostraram que, relativo a um oráculo aleatório, uma Máquina de Turing quântica deve levar tempo exponencial para resolver problemas NP-completo. Isso aparenta excluir a possibilidade de considerar um algoritmo quântico eficiente para um problema NP-completo, impedindo uma grande descoberta na teoria da complexidade computacional. Também foi mostrado que um limite inferior exponencial foi estabelecido no problema de inverter uma permutação aleatória (portanto, abrindo a possibilidade de funções quânticas "one-way"). Ambos resultados foram provados usando um argumento híbrido. Duas outras técnicas para estabelecer limites inferiores foram introduzidas. A primeira é o método dos polinômios [6], que foi usada para dar um limite inferior linear seguro na complexidade quântica da função "parity"no modelo da caixa preta. No mesmo artigo, foi mostrado que, em geral, a complexidade da consulta quântica de alguma função total no modelo da caixa preta está limitado pela sexta potência da complexidade da consulta determinística. A segunda técnica é o método dos adversários quânticos [3]. Essa técnica aparenta ser bem geral, e tem sido usada para obter limites seguros para uma variedade de problemas. Em particular, ela foi usada para provar um limite seguro no problema de inverter uma permutação aleatória.

9.4 BQP ⊆ NP?

Vamos começar essa seção definindo a classe MA.

Seja Merlin uma MT com recursos computacionais ilimitados, ou seja, Merlin é um oráculo que resolve problemas pertencentes à NP com custo de tempo unitário. Arthur é uma MT probabilística, e resolve problemas pertencentes à classe BPP eficientemente. Merlin então envia a Arthur um problema de decisão cuja resposta é "sim" e adicionalmente envia a resposta (instância) que resolve tal problema. Mas Merlin pode estar mentindo, e a resposta pode ser "não". Arthur deve então verificar a resposta em tempo probabilístico polinomial (BPP), então:

- Se a resposta para o problema for "sim", então Merlin estava falando a verdade, a resposta realmente existe e, com alta probabilidade, Arthur

conseguirá descobrir que Merlin estava falando a verdade.

- Se a resposta para o problema for "não", então Merlin estava mentindo, a resposta não existe e, com alta probabilidade, Arthur conseguirá descobrir que Merlin estava mentindo.

Ou seja, Arthur sempre descobre se Merlin estava mentindo ou não com alta probabilidade.

Essa maneira de resolver problemas chamamos de *protocolo Merlin-Arthur*.

Definição 9.4.1. *A **classe MA**[2] (Merlin-Arthur) é a classe dos problemas que são resolvidos pelo protocolo Merlin-Arthur.*

BQP $\subseteq$ NP? Como BQP inclui a habilidade da aleatoriedade, a melhor maneira de perguntar sobre isso é se BQP está contido em MA — a generalização probabilística da NP. Há indicações de que a resposta é negativa, visto que o problema da amostragem recursiva de Fourier, o qual tem um eficiente algoritmo quântico, não está em MA relativo a um oráculo. A principal questão que continua em aberto é se $BQP \subseteq MA$.

Talvez a peça-chave da teoria da complexidade clássica seja o teorema de Cook-Levin, que diz que 3-SAT é NP-completo. Recentemente, Kitaev provou o análogo quântico desse resultado. Ele mostrou que o problema dos "Hamiltonianos locais", que é a generalização natural do 3-SAT é completo para BQNP[3]. Uma consequência não trivial que segue desse fato é que $BQNP \subseteq P^{\#P}$. Nossa exposição desses resultados é baseado nos manuscritos. Nós não sabemos de nenhum exemplo, com excessão dos "Hamiltonianos locais", de problemas completos para o análogo quântico de NP. Desenvolver essa teoria é uma importante questão aberta na teoria da complexidade quântica.

[2]Em algumas referências, a classe MA é denotada como BPP^{NP}, que até seria uma forma mais intuitiva de denotar a classe, no entanto, a analogia à Merlin-Arthur é uma tradição nessa área.

[3]BQNP é denotado também como QMA (*Quantum Merlin-Arthur*), que é a classe análoga quântica da classe MA.

Referências Bibliográficas

[1] Church A. A note on the Entscheidungsproblem. *Journal of Symbolic Logic*, 1:40–41 and 101–102, 1936.

[2] R. L. Rivest; A. Shamir ; L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *CACM*, 21(2):120–126, February 1978.

[3] A. Ambainis. Quantum lower bounds by quantum arguments. In ACM, editor, *Proceedings of the thirty second annual ACM Symposium on Theory of Computing: Portland, Oregon, May 21–23, [2000]*, pages 636–643, New York, NY, USA, 2000. ACM Press.

[4] A. Barenco. Quantum physics and computers. *Contemp.Phys.*, 37(5), December 03 1996. Comment: 27 pages.

[5] A. Barenco, A.; Ekert. Dense coding based on quantum entanglement, 1994.

[6] R. et. al. Beals. Quantum lower bounds by polynomials. In IEEE, editor, *39th Annual Symposium on Foundations of Computer Science: proceedings: November 8–11, 1998, Palo Alto, California*, pages 352–361, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. IEEE Computer Society Press.

[7] J. S Bell. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, 1964.

[8] C. H.; et. al. Bennett. A suggested interpretation of the quantum theory in terms of hidden variables. *Physical Review Letters*, 70:1895–1899, 1993.

[9] S.J. Bennett, C.H.; Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69:2881–2884, 1992.

[10] U. Bernstein, E.; Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, October 1997.

[11] A. Berthiaume. Quantum computation. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 23–51. Springer-Verlag, Berlin Germany, 1997.

[12] D. Bohm. A suggested interpretation of the quantum theory in terms of hidden variables. *Physical Review*, 85, 1952.

[13] D.; et. al. Bouwmeester. Experimental quantum teleportation. *Nature*, 390:375–379, 1997.

[14] P.; Tapp A. Brassard, G.; Høyer. Quantum counting. *Lecture Notes in Computer Science*, 1443, 1998.

[15] Chen; Fulling; Chen. Generalization of grover's algorithm to multiobject search in quantum computing, part II: General unitary transformations. In Goong Chen and Ranee K. Brylinski, editors, *Mathematics of Quantum Computation, Chapman & Hall, 2002*. 2002.

[16] R. Cleve. An introduction to quantum complexity theory. *World Scientific*, June 28 1999.

[17] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In *Proc. Royal Society, A400, 97*, 1985.

[18] R. P. Feynman. Simulating physics with computers. *IJTP*, 21(6/7):467–488, 1982.

[19] M. A. Galindo, A.; Martin-Delgado. A family of grover's quantum searching algorithms. *Physical Review*, 2000.

[20] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, Philadelphia, Pennsylvania, 22–24 May 1996.

[21] E. M. Hardy, G. H.; Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1979.

[22] M. Hayward. Quantum computing and grover's algorithm. January22 2002.

[23] M. Hayward. Quantum computing and shor's algorithm. January22 2002.

[24] D. E. Knuth. *The Art of Computer Programming, vol.2*. Addison-Wesley series in computer science and information processing. Addison-Wesley, 1981.

[25] S. J. Lomonaco Jr. A talk on quantum cryptography, or how alice outwits eve. *AMS PSAPM Short Course*, pages 144–174, February 02 1999.

[26] S. J. Lomonaco Jr. A rosetta stone for quantum mechanics with an introduction to quantum computation. *AMS PSAPM Short Course*, July 17 2000.

[27] G. E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, 1965.

[28] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, New York, 1994.

[29] W. Rieffel, E. G.; Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, January 18 2000. Comment: 45 pages.

[30] A. Einstein; B. Podolsky; N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[31] M. Agrawal; N. Kayal; N. Saxena. PRIMES is in P. Report, Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur-208016, India, aug 2002.

[32] P. W. Shor. Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. *Lecture Notes in Computer Science*, 877, 1994.

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

[34] M. Boyer; G. Brassard; P. Høyer; A. Tapp. Tight bounds on quantum searching. *Los Alamos preprint*, 1996.

[35] A. Tartaglia. Is the epr paradox a paradox? *European Journal of Physics*, 1998.

[36] A.M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, Series 2(42):230–265, 1936-1937.

[37] N. J. Cerf; L.K. Grover; C.P. Williams. Nested quantum search and np-complete problems. *Los Alamos preprint*, 1998.

[38] A. C. Yao. Quantum circuit complexity. In *34th Annual Symposium on Foundations of Computer Science*, pages 352–361, Palo Alto, California, 3–5 November 1993. IEEE.